

## Sieci LAN, MAN i WAN - protokoły komunikacyjne



Wydawnictwo  
Fundacji Postępu Telekomunikacji

### Spis treści

darmowe ebooki

aktualne czasopisma



Wstęp .....	1
<b>1 Ogólna charakterystyka sieci komputerowych .....</b>	<b>3</b>
1.1 Podstawowe cele tworzenia sieci komputerowych .....	4
1.2 Klasyfikacja sieci komputerowych .....	4
1.3 Warstwowe architektury sieciowe .....	9
1.3.1 Krótka charakterystyka warstw modelu ISO-OSI .....	10
1.3.2 Architektura SNA .....	17
1.3.3 Architektura DNA.....	23
1.3.4 Architektura TCP/IP .....	30
1.3.5 Perspektywy rozwoju architektur sieciowych .....	51
<b>2 Warstwa łącza danych - podstawowe funkcje i usługi .....</b>	<b>54</b>
2.1 Metody sterowania przepływem ramek w WŁD i ocena ich jakości...	57
2.1.1 Charakterystyka ogólna algorytmów ARQ .....	58
2.1.2 Protokół <i>Stop-And-Wait</i> (SAW) .....	59
2.1.3 Protokoły okienkowe .....	61
2.1.3.1 Protokół <i>Go-Back-N</i> (GBN) .....	63
2.1.3.2 Protokół z selektywną retransmisją (SR).....	65
2.1.4 Ocena jakości protokołu SAW oraz protokołów okienkowych .....	67
2.1.4.1 Jakość protokołu <i>Stop-And-Wait</i> .....	67
2.1.4.2 Jakość protokołów okienkowych .....	70
2.2 Ogólna charakterystyka metod arbitracji dostępu do medium komunikacyjnego - klasyfikacja protokołów podwarstwy MAC .....	75
<b>3 Protokoły warstwy łącza danych w sieciach rozległych WAN.....</b>	<b>78</b>
3.1 Systemy z przepłytwaniem.....	81
3.1.1 Przepływanie określone (indywidualne) .....	82
3.1.2 Przepływanie z przekazywaniem przepustki.....	82
3.1.3 Uproszczona analiza jakości systemu z przepłytwaniem indywidualnym.....	83
3.2 BISYNC (BSC) - Protokół ze znakami sterującymi .....	85
3.2.1 Podstawowe zasady pracy protokołu .....	85
3.2.2 Format ramki .....	86
3.2.3 Wykrywanie błędów w transmisji.....	88
3.2.4 Ramkowanie i synchronizacja transmisji.....	88
3.2.5 Przykładowe procedury sterowania transmisją ramek .....	90

3.3 Protokół znakowy DDCMP z liczeniem znaków .....	92	4.2.5 Protokół dostępu do sieci pętlowej z rejestrami przesuwającymi .....	171
3.3.1 Podstawowe zasady pracy protokołu .....	92	4.2.6 Szybkie sieci LAN .....	173
3.3.2 Format ramki .....	93	4.2.6.1 100VG-AnyLAN .....	174
3.3.3 Wykrywanie błędów .....	94	4.2.6.1.1 Struktura sieci 100VG-AnyLAN .....	174
3.3.4 Synchronizacja i testowanie pracy stacji.....	96	4.2.6.1.2 Hub 100VG-AnyLAN .....	176
3.4 Protokół bitowy SDLC .....	96	4.2.6.1.3 Model ISO/OSI a standard 100VG-AnyLAN.....	176
3.4.1 Podstawowe zasady pracy.....	96	4.2.6.1.4 Priorytetowy dostęp do medium .....	178
3.4.2 Format ramki .....	96	4.2.6.1.5 Trening połączenia .....	180
3.4.3 Wykrywanie błędów i odtwarzanie ramek.....	98	4.2.6.1.6 Przygotowanie ramki MAC .....	181
3.5 Protokół bitowy HDLC .....	99	4.2.6.1.7 Podwarstwa PMI .....	181
3.5.1 Podstawowe informacje .....	99	4.2.6.1.8 Warstwa PMD .....	183
3.5.2 Konfiguracje logiczne HDLC .....	99	4.2.6.1.9 Przykładowy przebieg transmisji danych w sieci 100VG-AnyLAN.....	185
3.5.3 Stany logiczne i tryby pracy.....	101	4.2.6.2 Fast Ethernet.....	187
3.5.4 Format ramki .....	103	4.2.6.2.1 Topologia sieci ethernetowej .....	188
3.5.5 Rodzaje i funkcje ramek stosowanych w HDLC .....	104	4.2.6.2.2 Auto-Negocjacja.....	192
3.5.6 Fazy w pracy stacji .....	107	4.2.6.3 Porównanie technologii 100VG-AnyLAN i Fast Ethernet oraz innych rozwiązań sieci lokalnych.....	195
3.5.7 Przykład funkcjonowania HDLC .....	108	4.2.6.4 Gigabitowy Ethernet .....	196
3.5.8 Sterowanie przepływem i wykrywanie błędnych ramek .....	109	4.2.7 IsoEthernet IEEE 802.9 - multimedialny LAN.....	198
3.5.9 Klasifikacja protokołów typu HDLC .....	111	4.2.7.1 Topologia sieci .....	198
3.5.9.1 LAPB .....	113	4.2.7.2 Układy dostępu AU .....	199
3.5.9.2 LAPD.....	118	4.2.7.3 Architektura sieci IsoEthernet.....	200
<b>4 Przewodowe sieci LAN i MAN.....</b>	<b>122</b>	4.2.7.4 Tryby pracy IsoEthernetu .....	202
4.1 Podwarstwa kanału logicznego - LLC .....	124	4.2.7.5 Warstwa fizyczna IsoEthernetu .....	202
4.1.1 Adresy w sieciach LAN .....	129	4.2.7.6 Tryby pracy sieci IsoEthernet a warstwa fizyczna .....	203
4.2 Podwarstwa dostępu do medium MAC.....	132	4.2.7.7 Algorytm sygnalizacyjny autonegoacji .....	204
4.2.1 Protokół rywalizacyjny CSMA/CD - Standard IEEE 802.3 .....	133	4.2.7.8 Procedury sygnalizacyjne w kanale C.....	205
4.2.1.1 Podstawowe parametry techniczne .....	134	4.2.7.9 IsoEthernet a ATM .....	207
4.2.1.2 Struktura ramki podwarstwy MAC .....	137	4.2.7.10 Aplikacje multimedialne w IsoEtherencie .....	208
4.2.1.3 Zasady transmisji .....	138	4.2.7.11 Kierunki rozwoju IsoEthernetu .....	209
4.2.1.4 Wykrywanie kolizji.....	138	<b>4.2.8 FDDI - Protokół dostępu do medium światłowodowego             w sieci MAN .....</b>	209
4.2.1.5 Ocena jakości pracy sieci LAN z protokołem CSMA/CD .....	139	4.2.8.1 Podstawowe parametry .....	209
4.2.2 Protokół tokenowy dla sieci magistralowej - Standard IEEE 802.4 .....	144	4.2.8.2 Topologia sieci i typy stacji .....	211
4.2.2.1 Podstawowe parametry .....	144	4.2.8.3 Niezwodność pracy sieci.....	215
4.2.2.2 Format ramki w sieci magistralowej z tokenami.....	145	4.2.8.4 Warstwa fizyczna w FDDI.....	216
4.2.2.3 Zasady transmisji .....	147	4.2.8.5 Podwarstwa MAC.....	217
4.2.3 Protokół tokenowy dla sieci pętlowej - Standard IEEE 802.5 .....	154	4.2.8.6 Format tokena i ramki.....	219
4.2.3.1 Podstawowe dane techniczne.....	154	4.2.8.7 Ważniejsze zmienne, liczniki i flagi stosowane w procedurach FDDI.....	222
4.2.3.2 Format ramki i tokena.....	155	4.2.8.8 Protokół wymiany informacji w FDDI .....	224
4.2.3.3 Procedury transmisji .....	158		
4.2.3.4 Realizacja priorytetowego dostępu do pętli.....	161		
4.2.3.5 Ocena jakości pracy sieci pętlowej .....	166		
4.2.4 Protokół dla sieci pętlowej z wirującymi szczelinami (ramki).....	169		

**5 Bezprzewodowe sieci LAN i systemy satelitarne VSAT .....** **278**

5.1 Sieć i protokół dostępu ALOHA.....	279
5.1.1 Formaty ramek.....	279
5.1.2 Algorytmy dostępu ALOHA i zasady wymiany informacji w sieci ALOHA.....	280
5.1.3 Uproszczona analiza jakości protokołu ALOHA.....	281
5.1.4 Założenia ogólne i jakość protokołu S-ALOHA.....	284
5.1.5 Uwagi na temat stabilności protokołów typu ALOHA .....	286
5.2 Algorytmy dostępu typu CSMA i ich przykładowa implementacja .....	287
5.2.1 Zasady funkcjonowania algorytmów ze śledzeniem nośnej - CSMA ..	287
5.2.2 Przykładowa implementacja protokołu CSMA.....	289
5.2.3 Wybrane wyniki analizy algorytmów CSMA .....	290
5.3 Rozproszony algorytm dostępu podwarstwy MAC dla bezprzewodowej sieci LAN - Standard DFWMAC IEEE 802.11.....	292
5.3.1 Podstawowe cechy standardu IEEE 802.11 .....	293
5.3.2 Protokół DFWMAC dla komunikacji asynchronicznej DCF.....	295
5.3.2.1 Algorytm DCF.....	297
5.3.2.2 Algorytm rywalizacji o dostęp do medium i realizacji retransmisji ramek (ang. <i>Access Backoff Procedure</i> ).....	299
5.3.3 Protokół PCF dla obsługi ruchu synchronicznego .....	300
5.3.4 Struktury ramek w IEEE 802.11 .....	303
5.3.5 Jakość oferowanych usług .....	307

5.4 Standard ETSI - HIPERLAN dla radiowych sieci LAN .....	308
5.4.1 Podstawowe funkcje i usługi oferowane przez HIPERLAN .....	309
5.4.2 Typy ramek definiowanych przez protokół HIPERLAN CAC .....	313
5.4.3 Algorytm niewymuszonego priorytetowego dostępu do medium - NPMA .....	315
5.5 Systemy satelitarne VSAT .....	319
5.5.1 Konfiguracje fizyczne sieci VSAT .....	320
5.5.2 Organizacja transmisji w sieci VSAT .....	322
5.5.3 Architektura komunikacyjna sieci VSAT .....	323
5.5.4 Schemat komunikacji w typowej sieci VSAT o architekturze gwiazdy .....	328
5.5.5 Obszary zastosowań sieci VSAT i ich przykładowe aplikacje .....	329
5.5.6 Algorytmy dostępu do kanału satelitarnego .....	332
5.5.6.1 Metody stałego przydziału zasobów .....	334
5.5.6.2 Metody losowego przydziału zasobów .....	334
5.5.6.3 Metody przydziału zasobów na żądanie .....	336
5.5.7 Przyszłość sieci VSAT .....	337
6 Standardy dla rozległych sieci pakietowych: X.25 i Frame Relay .....	338
6.1 Protokół X.25 .....	338
6.1.1 Warstwowa architektura X.25 .....	339
6.1.2 Łącze wirtualne i kanał logiczny .....	341
6.1.3 Jednostki danych w X.25 .....	342
6.1.4 Procedury komunikacyjne w X.25 .....	343
6.1.4.1 Zestawianie, kasowanie (likwidacja) i restartowanie połączeń .....	343
6.1.4.2 Transmisja danych użytkownika .....	345
6.1.4.3 Kontrola przepływu danych .....	345
6.1.4.4 Sterowanie przepływem .....	346
6.1.4.5 Adresowanie .....	347
6.1.4.6 Udogodnienia .....	347
6.1.4.7 Przebieg połączenia w X.25 .....	347
6.1.4.8 Komutacja pakietów w sieci X.25 .....	350
6.1.4.9 Łączenie X.25 z innymi sieciami .....	351
6.2 Podstawy Standardu Frame Relay .....	352
6.2.1 Standaryzacja Frame Relay .....	352
6.2.2 Frame Relay Forum .....	354
6.2.3 Frame Relay jako jedna z technologii przełączania pakietów .....	355
6.2.4 Zastosowanie sieci FR .....	356
6.2.5 Ewolucja w kierunku ATM .....	357
6.2.6 Struktura połączeń w sieci Frame Relay .....	358
6.2.7 Adresowanie w sieci Frame Relay .....	359
6.2.8 Komutacja pakietów .....	360
6.2.9 Mechanizm informowania o przeciążeniu .....	362

6.2.10 Struktura ramki FR .....	363
6.2.11 Organizacja usług FR.....	364
<b>7 Asynchroniczny przekaz danych - ATM.....</b>	<b>366</b>
7.1 Architektura B-ISDN ATM .....	366
7.2 Warstwa fizyczna .....	369
7.2.1 Rodzaje interfejsów fizycznych.....	370
7.3 Warstwa ATM.....	372
7.3.1 Połączenia typu kanału logicznego i ścieżki logicznej .....	372
7.3.2 Komórka ATM .....	374
7.3.3 Sterowanie dostępem i zarządzanie zasobami sieci B-ISDN ATM ....	376
7.3.4 Kategorie i klasy usług warstwy ATM.....	385
7.4 Warstwa adaptacyjna ATM .....	389
7.4.1 Typy protokołów warstwy AAL .....	390
7.5 Połączenia w sieci ATM .....	392
7.5.1 Routing w sieciach ATM .....	393
7.5.2 Rodzaje połączeń w sieci ATM .....	397
7.6 Przyszłość ATM.....	400
<b>8 Wersja 6 protokołu IP .....</b>	<b>403</b>
8.1 Internetowy protokół IP .....	403
8.2 Podstawowe cechy protokołu IPv6 .....	404
8.3 Adresacja w protokole IPv6 .....	407
<b>9 Łączenie sieci - przegląd metod i układów pośredniczących .....</b>	<b>411</b>
9.1 Przykłady wzajemnego niedopasowania rozwiązań sieciowych w wybranych standardach sieci LAN i MAN.....	412
9.2 Sposoby łączenia sieci LAN .....	415
9.3 Urządzenia pośredniczące w łączeniu sieci .....	418
9.3.1 Regeneratory i proste urządzenia przełączające .....	419
9.3.2 Mosty .....	423
9.3.2.1 Koncepcja pracy mostów.....	424
9.3.2.2 Typy mostów .....	427
9.3.2.3 Podstawowe funkcje mostów przeźroczystych .....	428
9.3.2.4 Klasifikacja mostów przeźroczystych .....	429
9.3.2.4.1 Most przeźroczysty prosty .....	429
9.3.2.4.2 Most przeźroczysty uczący się .....	430
9.3.2.4.3 Most z algorytmem drzewa opinającego .....	432
9.3.2.4.4 Problemy związane ze stosowaniem mostów przeźroczystych.....	439
9.3.2.4.5 Most odległy.....	441
9.3.2.5 Source Routing .....	442
9.3.2.6 Porównanie mostów przeźroczystych i źródłowych .....	445

9.3.2.7 Mosty SRT.....	446
9.3.3 Przełączniki sieciowe i huby przełączające .....	446
9.3.3.1 Różnice pomiędzy mostem i przełącznikiem .....	448
9.3.3.2 Routery a przełączniki .....	450
9.3.3.3 Tryby pracy przełączników i metody przełączania.....	451
9.3.3.4 Architektura przełącznika .....	453
9.3.3.5 Praktyczne zastosowania przełączników .....	454
9.3.3.6 Zalety przełączników .....	458
9.3.3.7 Sieci wirtualne VLAN .....	459
9.3.3.8 Podsumowanie .....	461
9.3.4 Routery .....	461
9.3.4.1 Zadania routerów .....	461
9.3.4.2 Klasifikacje routerów .....	463
9.3.4.3 Protokoły wyboru trasy.....	464
9.3.4.3.1 Algorytmy i tablice routingu.....	465
9.3.4.3.2 Routing w sieciach TCP/IP.....	470
9.3.4.3.2.1 Podsieci .....	473
9.3.4.3.2.2 Nadsieci.....	474
9.3.4.3.2.3 Protokoły routingu stosowane w sieciach TCP/IP..	474
9.3.4.4 Routery w sieciach Novell .....	486
9.3.4.5 Koncepcja routingu w modelu ISO-OSI .....	487
9.3.4.5.1 Zasady adresacji ISO .....	487
9.3.4.5.2 Protokół IP OSI .....	488
9.3.4.5.3 IP-OSI routing .....	489
9.3.5 Bramy/konwertery protokołów .....	490
<b>10 Współpraca pakietowych sieci komputerowych z siecią ATM.....</b>	<b>492</b>
10.1 Wspieranie protokołu IP przez sieci ATM.....	494
10.1.1 Klasyczna wersja protokołu IP over ATM (IPoATM) – RFC 1577..	494
10.1.1.1 Enkapsulacja pakietów (LLC/SNAP) .....	495
10.1.1.2 Odwzorowanie sieci ATM w logiczną sieć IP – definicja podsieci LIS .....	495
10.1.1.3 Rozwiązywanie problemu adresowania.....	497
10.1.1.3.1 Połączenia PVC .....	497
10.1.1.3.2 Połączenia SVC – serwery ATMARP .....	498
10.1.1.3.3 Format pakietów ATMARP i InATMARP .....	499
10.1.1.4 Proces nawiązywania połączenia wewnętrz sieci LIS .....	500
10.1.1.5 Routery w ATM – łączenie stacji należących do różnych LIS .....	500
10.1.2 Rozszerzenia standardu Classical IP over ATM .....	501
10.1.2.1 NHRP – bezpośrednie połączenia między sieciami IP, opartymi na tej samej platformie ATM .....	502
10.1.2.1.1 Serwery NHS .....	502

10.1.2.1.2 Zasada działania protokołu NHRP .....	503
10.1.2.1.3 Bezpieczeństwo i ograniczenia protokołu NHRP .....	503
10.1.2.2 MARS – multicasting i broadcasting w IPoATM .....	504
10.1.2.2.1 Wysyłanie informacji do grupy użytkowników .....	505
10.1.2.2.2 Dołączanie i usuwanie stacji z grupy .....	506
10.2 Emulacja sieci LAN w sieciach ATM .....	506
10.2.1 Elementy LANE .....	508
10.2.2 Połączenia funkcjonujące w LANE .....	511
10.2.3 Opis funkcjonowania elementów LANE .....	513
10.2.4 Algorytm drzewa opinającego w protokole LANE .....	518
10.2.5 Inteligentny serwer BUS .....	519
10.2.6 Łączenie segmentów sieci LAN .....	519
10.2.7 LANE w środowisku sieci Token Ring .....	520
10.2.8 Uwagi końcowe .....	521
10.3 Współpraca sieci Frame Relay i ATM .....	522
10.3.1 Scenariusze współpracy sieci Frame Relay i ATM .....	522
10.3.2 Funkcje IWF .....	524
<b>11 Uwagi końcowe i wskazówki bibliograficzne .....</b>	<b>528</b>
<b>Bibliografia .....</b>	<b>531</b>
<b>Zestawienie skrótów teleinformatycznych .....</b>	<b>535</b>
<b>Słownik terminów teleinformatycznych .....</b>	<b>546</b>

## Wstęp

Ostatnie dwa dziesięciolecia były okresem burzliwego rozwoju telekomunikacji cyfrowej i różnorodnych systemów komputerowych. Przyczynił się do tego zarówno rozwój technik informatycznych i technologii układów scalonych VLSI, jak też coraz powszechniejsze stosowanie nowoczesnych, szerokopasmowych mediów transmisyjnych. Stworzono efektywne języki programowania i systemy operacyjne, opracowano nowe typy mikroprocesorów, pamięci operacyjnych i pamięci masowych oraz wprowadzono do powszechnego użytku łączna światłowodowe i kanały satelitarne. Wszystkie te czynniki miały też swój istotny wpływ na dynamiczny rozwój sieci komputerowych, zarówno rozległych, obejmujących swoim zasięgiem poszczególne kraje i całe kontynenty, jak i lokalnych, zaspakających potrzeby jednej instytucji. Obserwując zmiany zachodzące w telekomunikacji, mikroelektronice i informatyce można przewidywać, że kolejna dekada będzie okresem szczególnego rozwoju sieci świadczących usługi multimedialne oraz różnorodnych systemów łączności bezprzewodowej, zarówno zintegrowanych systemów radiokomunikacji komórkowej - naziemnych bądź satelitarnych - jak też systemów łączności osobistej i bezprzewodowych sieci lokalnych.

Sieci komputerowe, bez względu na ich rozległość i świadczone usługi, są systemami bardzo skomplikowanymi. Prawidłowe ich funkcjonowanie wymaga więc uzgodnienia zasad zarówno wymiany informacji na różnych poziomach ogólności, jak też sposobu prezentacji przesyłanych wiadomości. W celu uproszczenia zasad projektowania i implementacji systemów teleinformatycznych ich oprogramowanie sieciowe ma zazwyczaj modularną, warstwową architekturę, a poszczególne warstwy realizują ściśle określone funkcje. Warstwy dolne tzw. warstwy komunikacyjne, realizowane częściowo sprzętowo, są we wszystkich logicznych architekturach sieciowych odpowiedzialne za niezawodny przekaz informacji poprzez sieć komunikacyjną. Z kolei warstwy górne wspomagają realizację usług aplikacyjnych.

*Celem niniejszej książki jest prezentacja wybranych protokołów komunikacyjnych, opis zasad ich funkcjonowania oraz przedstawienie podstawowych parametrów charakteryzujących jakość tych protokołów. Przedmiotem naszego zainteresowania są głównie protokoły warstwy łączącej danych i warstwy sieciowej, zarówno te znajdujące szerokie zastosowanie praktyczne, jak i przykłady typowo dydaktyczne prezentujące ogólne koncepcje dostępu do medium transmisyjnego oraz zasady i mechanizmy sterowania przepływem danych.* Omawiane protokoły ilustrują metody wymiany jednostek danych w sieciach zarówno z transmisją typu punkt-punkt, charakterystyczną dla sieci rozległych, jak też

punkt-wielopunkt, realizowaną w sieciach lokalnych z medium umożliwiającym transmisję rozgłoszeniową. W odniesieniu do większości algorytmów sterowania przepływem ramek w warstwie łączą danych oraz metod dostępu do medium obok ich opisu zamieszczono uproszczone analizy jakości ich funkcjonowania oraz przykładowe zależności pomiędzy podstawowymi parametrami sieci. Pozwalają one na wszechstronną ocenę opisywanych protokołów oraz wybór rozwiązań dostosowanych do konkretnych potrzeb użytkowników. Przegląd metod sterowania przepływem danych, wraz z oceną ich efektywności, a także opisy podstawowych protokołów warstwy łączą danych stosowanych w sieciach rozległych znajdują się w rozdziałach 2 i 3 książki.

Z uwagi na duże i stale rosnące zainteresowanie szybkimi technologiami i technikami komutacyjnymi, jak też nowymi standardami komunikacyjnymi opracowanymi dla sieci publicznych WAN, szybkich sieci LAN i MAN oraz systemów łączności bezprzewodowej, zagadnieniem tym poświęcimy w książce sporo uwagi. Problematyka ta będzie przedmiotem rozważań zawartych w rozdziałach od 4 do 8.

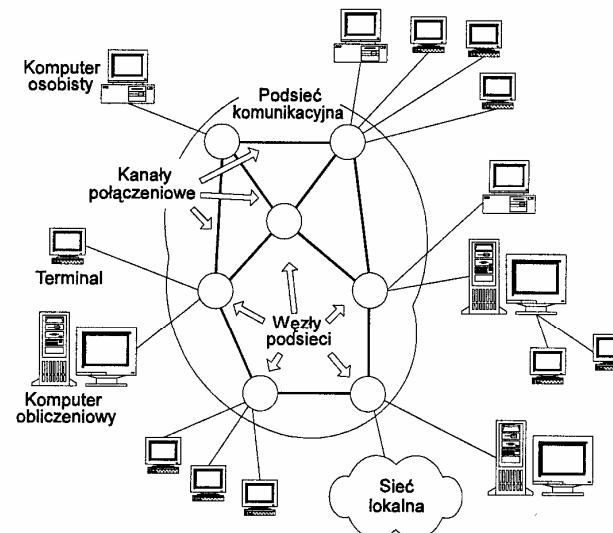
Większość użytkowników i administratorów sieci, w szczególności sieci lokalnych, jest zainteresowanych rozbudową bądź też integracją swoich sieci. Coraz powszechniejsze jest bowiem tworzenie sieci korporacyjnych. Zgłasiane jest też zapotrzebowanie na szybki dostęp do specjalizowanych usług i nowych aplikacji sieciowych. Możemy to zagwarantować zarówno poprzez sprzętową rozbudowę sieci LAN jak też łączenie tych sieci za pomocą sieci MAN i WAN. Tym nowym problemom rozbudowy i integracji sieci zostaną poświęcone dwa ostatnie rozdziały książki.

Przed przystąpieniem do prezentacji poszczególnych standardów sieciowych i protokołów komunikacyjnych w rozdziale 1 książki, przedstawimy najistotniejsze cechy sieci komputerowych. Zaprezentujemy podstawowe cele ich tworzenia jak i przykładowe aplikacje sieciowe. Wskażemy też na potrzebę standaryzacji sprzętu i oprogramowania sieciowego odpowiedzialnego za wymianę informacji między użytkownikami. Dokonamy także krótkiego przeglądu warstwowych architektur sieciowych i zdefiniujemy podstawowe funkcje realizowane przez poszczególne warstwy tych architektur, realizowane sprzętowo lub programowo. Przytoczymy też najistotniejsze definicje realizowanych operacji elementarnych i usług świadczonych przez poszczególne warstwy.

Niniejsza książka przeznaczona jest dla szerokiego grona odbiorców. Stanowić ona może materiał do wstępnych studiów na temat organizacji i pracy sieci komputerowych. Opisy i załączone ilustracje czynią z niej kompendium wiedzy przydatne zarówno dla studentów jak i potencjalnych użytkowników bądź administratorów sieci komputerowych, w szczególności sieci LAN i MAN.

## 1 Ogólna charakterystyka sieci komputerowych

*Sieci komputerowe są definiowane zwykle jako zbiory autonomicznych komputerów (oraz innych urządzeń końcowych) połączonych wzajemnie podsiecią komunikacyjną tworzoną przez węzły komunikacyjne tj. specjalizowane komputery (ang. nodes lub Interface Message Processors - IMPs) i kanały połączeniowe.* Przykładową strukturę sieci komputerowej ilustruje rysunek 1.1. Węzły i kanały połączeniowe tworzą przy tym podsystem dystrybucji informacji. Z kolei komputery obliczeniowe i inne urządzenia końcowe sieci stanowią elementy podsystemów przetwarzania informacji i dostępu do zasobów sieciowych. Sieci komputerowe zaczęto tworzyć w latach sześćdziesiątych. Spektakularnym przykładem sieci z tego okresu jest sieć ARPA (ang. Advanced Research Project Agency), rozwijana i normowana przez Departament Obrony USA, w której po raz pierwszy zastosowano komutację pakietów (ang. packet switching). W metodzie tej, w przeciwieństwie do tradycyjnej metody zestawiania połączenia, tj. komutacji kanałów (ang. circuit switching) - charakterystycznej dla systemów telefonicznych - pakiety/wiadomości mogą być buforowane w węzłach pośrednich i przesyłane z opóźnieniem w kierunku stacji docelowej (zgodnie z zasadą store-and-forward).



Rys. 1.1. Przykładowa struktura sieci komputerowej z podsiecią komunikacyjną i urządzeniami końcowymi

## 1.1 Podstawowe cele tworzenia sieci komputerowych

*Głównym celem tworzenia sieci komputerowych jest zapewnienie efektywnego wykorzystania zasobów sprzętowych i programowych* będących w dyspozycji rozproszonych użytkowników oraz możliwość oferowania im różnorodnych usług, w tym najpopularniejszej usługi poczty elektronicznej. Połączenie autonomicznych komputerów w jeden "organizm" zapewnia **wielodostęp do różnorodnych baz danych i specjalizowanych programów**, umożliwiając szybkie i zdalne obliczenia. Sieć zapewnia też **właściwy podział obciążenia** pomiędzy różne komputery obliczeniowe.

Innym ważnym celem tworzenia sieci jest zagwarantowanie wyższej niezawodności usług poprzez zapewnienie istnienia w sieci alternatywnych źródeł informacji (baz danych), możliwości obliczeniowych i dróg połączeniowych.

Tworzenie sieci może też spowodować istotne **oszczędności finansowe** w pracy użytkowników sieci, szczególnie wtedy, gdy koszty jednostkowej transmisji są małe w porównaniu z jednostkowymi kosztami obliczeń. Ekonomiczne aspekty funkcjonowania sieci w istotnym stopniu wpłynęły na wyodrębnienie się ważnej grupy sieci komputerowych, nazywanej sieciami lokalnymi (ang. *Local Area Networks* - LANs). Komputery osobiste (ang. *Personal Computers* - PC) mają i średniej mocy obliczeniowej mają bowiem znacznie korzystniejszy od dużych komputerów obliczeniowych stosunek kosztów obliczeń do jakości realizowanych przez nie usług, tj. szybkości wykonywania obliczeń, pojemności pamięci, itp.

Ważnym elementem, branym pod uwagę przy tworzeniu sieci, szczególnie sieci rozproszonych na dużym obszarze (ang. *Wide Area Networks* - WANs), jest **zapewnienie przez sieć rozległego i rozprozonego medium komunikacyjnego**.

Budując sieć komputerową należy przy tym mieć na względzie możliwość realizacji w sieci określonych aplikacji i usług. W szczególności sieć winna zapewnić:

- zdalny dostęp do różnorodnych baz danych (serwisów informacyjnych, usług finansowych, informacji bibliotecznych, automatycznych gazet, itp.);
- zdalne aktualnianie programów i zdalne wykonywanie obliczeń, oferując specjalizowane programy, obliczenia realizowane on-line, podział zadań, itp.);
- organizację usług, telekonferencji, wideokonferencji, poczty elektronicznej, itp.

## 1.2 Klasifikacja sieci komputerowych

Opis zarówno cech charakterystycznych jak i możliwości oferowanych przez różne rozwiązania sieciowe realizowany jest zwykle w odniesieniu do określonych klas sieci komputerowych. *Podział sieci na klasy może być przy tym dokonywany między innymi w zależności od zasięgu terytorialnego sieci, typu podsieci komunikacyjnej, czy też rodzaju stosowanej w sieci techniki komu-*

*tacji. Z punktu widzenia zasięgu terytorialnego wyróżniamy sieci rozległe WAN, sieci lokalne LAN oraz sieci miejskie bądź metropolitalne MAN (ang. *Metropolitan Area Network*). Każdy z tych rodzajów sieci charakteryzuje się zespołem dość specyficznych atrybutów.*

*Rozległa sieć komputerowa WAN to sieć łącząca urządzenia znacznie oddalone od siebie geograficznie. Łączy ona ze sobą nie tylko pojedyncze komputery, ale również sieci lokalne i metropolitalne, bez ograniczeń narzuconych na odległość między nimi. Swoim zasięgiem obejmuje kraje, a nawet całe kontynenty (czyli setki-tysiące kilometrów), wynikiem czego mogą być znaczne opóźnienia propagacyjne (szczególnie w przypadku użycia łącz satelitarnych) orazwiększy koszt usług komunikacyjnych. Sieć WAN charakteryzuje się zwykle większą częstością występowania błędów oraz większą podatnością na uszkodzenia łącz transmisyjnych niż w typowych sieciach LAN i MAN. Przepływność informacji w takiej sieci jest z kolei znacznie mniejsza od przepustowości oferowanych przez sieci LAN i MAN, i mieści się w granicach od kilku kb/s do kilkudziesięciu Mb/s. Sieć typu WAN jest często wykorzystywana, zarówno przez osoby prywatne jak też różnego rodzaju instytucje i organizacje publiczne, do uzyskiwania dostępu do odległych baz danych bądź systemów przetwarzania informacji.*

*Lokalna sieć komputerowa LAN zawiera zwykle od kilku do kilkudziesięciu niezależnych urządzeń, nazywanych stacjami, rozmieszczonych na niewielkim obszarze (np. w laboratorium, biurze, instytucji) i połączonych za pośrednictwem fizycznych kanałów komunikacyjnych o niewielkich długościach. Komputery komunikujące się przez taką sieć posiadają podobne uprawnienia, a odległość pomiędzy parą stacji nie przekracza kilku kilometrów. W związku z tym, że stacje położone są blisko siebie, koszty budowy sieci są dużo mniejsze niż koszty instalacji sieci rozległej. Sieć LAN można też stosunkowo łatwo rozbudowywać. W sieciach tych szybkość transmisji informacji wzrasta, w stosunku do szybkości transmisji w sieciach WAN, kilka lub kilkadziesiątkrotnie, do wartości od 1 Mb/s do kilku Gb/s. Rośnie też niezawodność transmisji. Sieć LAN zapewnia użytkownikom dostęp do komputerów danej sieci, w tym korzystanie ze wspólnych pamięci operacyjnych i masowych, a także dostęp do drukarek, ploterów oraz możliwość korzystania z szeregu usług sieciowych. Najczęściej istnieje też możliwość dołączania sieci LAN do sieci rozległej i korzystania z dostępnych w niej usług.*

Trzecim rodzajem sieci jest metropolitalna sieć komputerowa MAN. Pod względem zasięgu jest ona siecią pośrednią między sieciami LAN i WAN. *Sieci MAN łączą węzły i stacje rozlokowane na obszarze o średnicy do około 50 km. Sieć MAN obejmuje więc swym zasięgiem obszar miasta lub osiedla, stąd często bywa nazywana siecią miejską. Szybkość transmisji w takiej sieci wynosi zwykle od kilku Mb/s do setek Mb/s.*

Biorąc pod uwagę typ podsieci komunikacyjnej wyróżniamy sieci z transmisją punkt-punkt, charakterystyczną dla sieci rozległych i sieci z transmisją

**rozsiewczą** bądź wielopunktową (ang. *broadcast, multipoint*), charakterystyczną dla sieci LAN, MAN oraz różnych rodzajów sieci radiowych i satelitarnych.

W przypadku rozległych sieci komputerowych informacje wymieniane pomiędzy użytkownikami końcowymi są przesyłane wewnątrz podsieci komunikacyjnej. Droga sygnału (bądź jednostki danych) jest w tym przypadku zestawem łączy i węzłów danej sieci. *Sposób zestawienia połączeń elektrycznych (czy też fizycznych) i ewentualnie logicznych w danej sieci komputerowej (czy ogólnie sieci telekomunikacyjnej) nazywamy techniką komutacji. W zależności od realizowanych w węzłach procedur mówimy zwykle o komutacji kanałów, komórek, pakietów bądź wiadomości.*

**Komutacja kanałów** jest metodą realizowaną przez większość systemów telefonii publicznej, zarówno stałej jak i ruchomej. Cechami charakterystycznymi tej techniki są: konieczność zestawiania (ustanawiania) połączenia przed zainicjowaniem przekazu danych oraz wyłączność pary komunikujących się systemów końcowych na użytkowanie zestawionego między nimi połączenia fizycznego. Inną cechą tej techniki jest brak dodatkowych opóźnień w przekazie danych w fazie „korespondencji”, poza opóźnieniami propagacyjnymi i opóźnieniami wynikającymi z szybkości transmisji w łączu.

**Pozostale**, wymienione powyżej, *metody komutacji charakteryzują się możliwością czasowego przechowywania informacji w węzłach podsieci komunikacyjnej, na trasie między stacjami źródłową i docelową.*

**Metoda komutacji wiadomości ma bardzo ograniczone znaczenie praktyczne.** Może być jednakże traktowana jako metoda źródłowa dla komutacji pakietów czy też komórek. W komutacji wiadomości cała przekazywana informacja jest buforowana w węźle tranzystowym przed jej wysłaniem do kolejnego węzła podsieci komunikacyjnej zgodnie z zasadą „zapamiętaj i przekaż” (ang. *store and forward*). Metoda komutacji wiadomości jest jednak mało elastyczna. W przypadku długich zbiorów danych może wprowadzać szereg niekorzystnych efektów, jak np. duże opóźnienia na skutek buforowania wiadomości w węzłach, przepełnianie pamięci węzłów itp. Te poważne mankamenty wyeliminowane zostały (przynajmniej częściowo) w pokrewnych metodach komutacji komórek i pakietów, poprzez wprowadzenie podziału wiadomości na mniejsze jednostki danych.

Najbardziej rozpowszechnioną techniką komutacyjną, stosowaną w sieciach komputerowych, jest **komutacja pakietów**. *W tym przypadku wiadomości dzielone są na bloki zwykłe o stałej długości (z wyjątkiem bloku ostatniego), do których dodane są części organizacyjne. Tworzona w ten sposób jednostka danych nazywana jest pakietem bądź datagramem. Identyczna zasada stosowana jest też w przypadku komutacji komórek. Zakłada się jednakże, iż długości komórek są znacznie krótsze od typowych długości pakietów.* W sieci pakietowej czyli w sieci z komutacją pakietów projektant lub administrator tej sieci narzuca zwykle ograniczenie od góry na wielkość jednostkowego bloku przesyłanych danych. Długość tego bloku może być różna dla różnych sieci.

Najczęściej pakiety najdłuższe zawierają kilka tysięcy bajtów, natomiast najkrótsze kilkadziesiąt bajtów. W przypadku „wytworzenia” przez proces aplikacyjny wiadomości dłuższej niż maksymalna długość pakietu, rodzi się potrzeba podziału wiadomości na mniejsze „porcje”, które następnie umieszczane są w pakietach i transmitowane przez sieć. *W sieciach komputerowych przekaz pakietów poprzedzany jest często zestawieniem tzw. połączenia wirtualnego (ang. virtual circuit). Oznacza to, że przed zainicjowaniem transmisji pakietów ma miejsce uzgodnienie całej trasy połączenia i przypisanie jej i jej fragmentom, numerów nazywanych identyfikatorami połączenia wirtualnego (ang. virtual circuit identifier).* Następujący, po tej fazie przekaz poszczególnych pakietów, danej wiadomości, realizowany jest wzduż danego połączenia wirtualnego, zgodnie z zasadą store and forward, typową dla komutacji pakietów. Możemy zatem mówić o komutacji pakietów bądź komórek realizowanej w połączeniu wirtualnym. Ten typ komutacji znajduje szerokie zastosowanie w pakietowych sieciach publicznych typu X25, Frame Relay czy też w sieci ATM.

*Odmienny charakter ma proces przekazu pakietów w sieciach świadczących tzw. usługi bezpośredniowe lub datagramowe. Przy tym typie przekazu pakietów, nazywanych wówczas datagramami nie jest wymagane wcześniejsze zestawienie ani połączenia fizycznego ani też połączenia wirtualnego.* Pakiety wchodzące w skład nawet tej samej wiadomości i wymieniane pomiędzy tymi samymi użytkownikami mogą docierać do adresata zupełnie odmiennymi drogami, w zależności od aktualnych warunków panujących w sieci (np. stopnia obciążenia lokalnych linii, zajętości buforów węzłów), realizowanych w sieci zasad obsługi pakietów, czy też przyjętej strategii routingu. *Ten typ komutacji określany jest mianem datagramowej komutacji pakietów (ang. datagram packet switching).*

Zalety wynikające ze stosowania komutacji pakietów to między innymi:

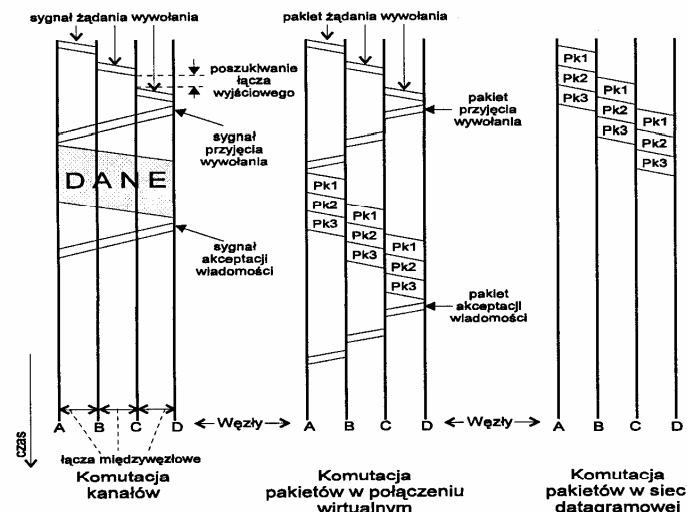
- możliwość zajmowania i zwalniania pasma medium komunikacyjnego zgodnie z rzeczywistymi potrzebami transmisyjnymi, a nie jak w przypadku komutacji kanałów - zajmowanie łącza na cały czas trwania połączenia,
- możliwość współużytkowania łącza przez pakiety pochodzące z różnych stacji źródłowych i kierowanych do różnych adresatów,
- możliwość naliczania opłat zgodnie z ilością przesłanych danych, a nie - z czasem trwania połączenia oraz zazwyczaj
- ograniczenie, w stosunku do komutacji wiadomości czasów buforowania wiadomości wielopakietowych w węzłach tranzystowych,
- możliwość obsługi ruchu interakcyjnego.

Komutacja pakietów rodzi też szereg poważnych problemów, nieznanych w komutacji kanałów. Są to między innymi:

- możliwość wystąpienia nagłego spiętrzenia ruchu na określonych trasach, prowadzącej do zablokowania węzłów i utraty pakietów, bądź dużych opóźnień w ich transmisji,

- możliwość wystąpienia zmiany kolejności w dostarczaniu pakietów do węzła docelowego.

Obie z negatywnych cech komutacji pakietów odnoszą się w zasadzie do podsystemów komunikacyjnych, realizujących bezpołączeniowy, czy też datagramowy, tryby pracy. W sieci z połączonymi wirtualnymi możemy bowiem mówić o rezerwacji zasobów w fazie zestawiania połączenia, a fakt zestawienia połączenia wirtualnego przed rozpoczęciem przekazu pakietów gwarantuje właściwą kolejność ich dostarczenia do adresata. Przykładowe diagramy czasowe, ilustrujące omówione powyżej techniki komutacji, pokazane są na rysunku 1.2.



Rys. 1.2. Ilustracja zależności czasowych dla różnych technik komutacji

Prawidłowe funkcjonowanie sieci komputerowych wymaga uzgodnienia szeregu zasad protokolarnych, a wymiana informacji między stacjami może odbywać się z udziałem lub bez udziału stacji nadzorującej ten proces. Sieć wykorzystująca stację główną (nadziedną/zarządzającą) (ang. *master*), nazywana jest w literaturze **siecią o strukturze hierarchicznej** (ang. *hierarchical network*). Stacja nadziedna zarządza i steruje pracą takiej sieci, a jej uszkodzenie może poważnie zakłócić działanie całej sieci. Przykładem sieci o strukturze hierarchicznej jest sieć IBM-SNA. Z kolei sieć, która nie posiada wyodrębnionej stacji zarządzającej, nazywana jest **siecią o strukturze rozproszonej** (ang. *distributed network*). Funkcje zarządzania i sterowania siecią są w tym przypadku rozłożone pomiędzy wszystkich użytkowników sieci (ang. *peer-to-peer network*). Uszkodzenie jednego z węzłów może wpływać w tym przypadku na pracę sieci jedynie w sąsiedztwie uszkodzonego węzła. Sieciami o strukturze rozproszonej są np. sieci Internet i DECnet. Zasady organizacji zarówno sieci SNA, Internet jak i DECnet zostaną szerzej omówione w następnym podrozdziale książki.

### 1.3 Warstwowe architektury sieciowe

**Współczesne sieci komputerowe zapewniają wzajemną współpracę różnorodnego sprzętu komputerowego.** Jest to efekt daleko posuniętej strukturalizacji i standaryzacji w zakresie oprogramowania i wyposażenia sprzętowego.

Standaryzacja stanowi niewątpliwie źródło korzyści zarówno dla użytkowników sieci jak też producentów. W kontekście stałej rywalizacji producentów korzyści użytkowników wynikają z podnoszenia jakości oferowanych wyrobów oraz propozycji nowych usług. Efektem konkurencji jest bowiem produkcja kompatybilnego i komplementarnego wyposażenia sieciowego. Dotyczy to w szczególności sprzętu i oprogramowania dla sieci LAN.

Aby ograniczyć złożoność sieci oraz umożliwić wzajemną komunikację heterogenicznego sprzętu komputerowego systemy sieciowe projektowane są w sposób strukturalny. Oznacza to, że różne funkcje odpowiedzialne za realizację przekazu informacji pomiędzy stacjami końcowymi zorganizowane są w postaci warstw. Całość oprogramowania sieciowego tworzy tzw. architekturę warstwową.

Pierwsze prace nad tworzeniem logicznych architektur warstwowych podjęte zostały na początku lat siedemdziesiątych. Główni producenci sprzętu komputerowego, firmy IBM i DEC, opracowały niezależnie i wyłącznie dla swoich potrzeb architektury sieciowe SNA (ang. *Systems Network Architecture*) i DNA (ang. *Digital Network Architecture*). Przygotowane pakiety oprogramowania zapewniły komunikację komputerów różnych typów produkowanych przez wyżej wymienione firmy (bez możliwości bezpośredniej współpracy SNA i DNA). Stan taki rodził poważne zagrożenie dla innych producentów sprzętu sieciowego, mogąc prowadzić do ich uzależnienia od potentatów komputerowych lub utraty znacznej części odbiorców, a w konsekwencji do monopolizacji rynku. W roku 1977 ISO (ang. *International Standards Organization*) powołała Komisję, której celem było opracowanie ogólnej koncepcji modelu warstwowej architektury sieciowej.

W chwili obecnej, wśród dużej grupy modeli architektur warstwowych, implementowanych w sieciach komputerowych, najistotniejsze znaczenie praktyczne, poza wymienionymi powyżej modelami ISO-OSI (ISO - *Open Systems Interconnection*), SNA i DNA, ma architektura TCP/IP (ang. *Transmission Control Protocol/Internet Protocol*). Specyficzna sytuacja, odnośnie oprogramowania sieciowego, ma miejsce w sieciach LAN, w których dla potrzeb lokalnej komunikacji stacji roboczych, urządzeń periferyjnych oraz tzw. serwerów aplikacji opracowano szeroki zestaw sieciowych systemów operacyjnych (ang. *Network Operating Systems* - NOS) dostosowanych do potrzeb i możliwości systemów operacyjnych DOS, OS/2 czy też UNIX.

Popularne architektury sieciowe takie jak model ISO-OSI, SNA, DNA czy też TCP/IP różnią się między sobą zarówno liczbą warstw, sposobem ich organizacji

jak też zasadami nawiązywania połączeń między stacjami sieci. Krótka charakterystyka podstawowych cech funkcjonalnych poszczególnych architektur będzie przedmiotem naszego zainteresowania w kolejnych paragrafach tego rozdziału.

Cechą charakterystyczną wszystkich architektur warstwowych, jak też w szczególności sieciowych systemów operacyjnych NOS dla sieci LAN jest to, że w tzw. warstwach komunikacyjnych, tj. odpowiedzialnych za przekaz informacji poprzez podsieć komunikacyjną, korzystają one z popularnych i powszechnie akceptowanych standardów sieciowych tworzonych przez IEEE (ang. *Institute of Electrical and Electronic Engineers*), ANSI (ang. *American National Standards Institute*), ETSI (ang. *European Telecommunications Standards Institute*), ITU-T (ang. *International Telecommunications Union*) (CCITT) czy też ISO. Standardy te będą obszernie omawiane w dalszych rozdziałach niniejszej książki.

### 1.3.1 Krótka charakterystyka warstw modelu ISO-OSI

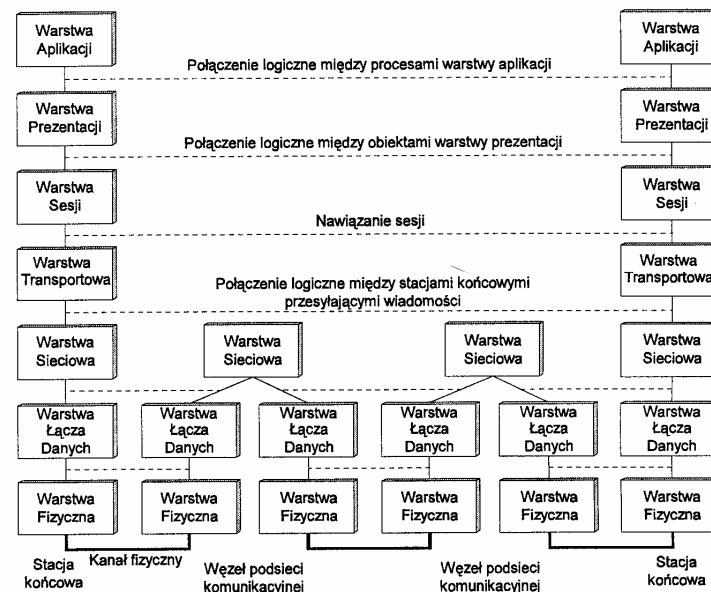
W pracach nad modelem warstwowym, nazywanym często modelem odniesienia, ISO kierowała się wieloma zasadami. Najważniejsze z nich można sformułować w sposób następujący:

- tworzenie oddzielnej warstwy może mieć miejsce, gdy wymaga tego poziom abstrakcji w prezentacji lub przekształcaniu informacji;
- każda warstwa winna realizować właściwie zdefiniowane funkcje;
- funkcje realizowane przez poszczególne warstwy winny uwzględniać powszechnie akceptowane standardy;
- liczba warstw powinna minimalizować ilość informacji przepływającej przez styki międzywarstwowe;
- ilość warstw nie powinna być jednocześnie zbyt mała by wyraźnie różnych funkcji nie umieszczać w tej samej warstwie.

W wyniku prac Komisji zdefiniowano zbiór funkcji, zasad i operacji podstawowych wymaganych przy współpracy sieciowej komputerów. Przyjęte przez ISO rozwiązanie nazwano siedmiowarstwowym otwartym modelem odniesienia (ang. *Open Systems Interconnection Reference Model*, OSI RM). Zaproponowana i rozpowszechniona przez ISO architektura pokazana jest na rysunku 1.3. Poszczególne warstwy modelu ISO OSI tj. fizyczna (ang. *physical*), łącza danych (ang. *data link*), sieciowa (ang. *network*), transportowa (ang. *transport*), sesji (ang. *session*), prezentacji (ang. *presentation*) i zastosowań/aplikacji (ang. *application*) realizują szereg różnorodnych funkcji nieodzownych dla prawidłowego funkcjonowania sieci.

Zgodnie z intencją projektantów **model ISO stanowi całościową, lecz otwartą propozycję architektury sieciowej, z której poszczególni administratorzy sieci (w zależności od konkretnej implementacji) dokonują stosownego wyboru oprogramowania warstw i realizowanych przez nie funkcji**. Poniżej podajemy przykładowe zadania warstw w modelu ISO.

#### 1.3.1 Krótka charakterystyka warstw modelu ISO-OSI



Rys. 1.3. Warstwowa architektura logiczna ISO-OSI z uwzględnieniem oprogramowania węzłów podsieci komunikacyjnej

**Warstwa fizyczna** (WF) zapewnia przekaz ciągów bitów (sygnałów elementarnych) między dwiema lub wieloma stacjami połączonymi bezpośrednio wspólnym medium komunikacyjnym. Warstwa ta definiuje styl sprzętowy oraz zasady, zgodnie z którymi bity przepływają między komunikującymi się stacjami. Styl ten opisują cztery charakterystyki: mechaniczna, elektryczna, funkcjonalna i proceduralna. Najpopularniejszym standardem warstwy fizycznej jest styl RS 232-C, umożliwiający połączenie stacji użytkownika z modemem (dołączonym do analogowego telefonicznego łącza rozmównego).

**Warstwa łącza danych** (WLD) ma za zadanie zapewnienie niezawodnego przekazu ramek danych przesyłanych kanałem cyfrowym wnoszącym zakłócenia; w szczególności do funkcji tej warstwy należy:

- tworzenie ramek informacyjnych/sterujących oraz wyznaczanie ciągów kontrolnych,
- wykrywanie błędów (ewentualnie ich korygowanie) i generowanie ramek powiadomień (ang. *acknowledgments*),
- sterowanie dostępem do medium komunikacyjnego.

Przykładami standardowych protokołów warstwy łącza danych (WLD) są dla sieci WAN z połączaniami typu punkt-punkt orientowane bitowo protokoły HDLC, SDLC i LAP-B. Z kolei, w przypadku sieci LAN będą to podstawowe standardy serii IEEE 802 (ISO 8802) oraz ANSI i ETSI.

**Warstwa sieciowa** (WŚ) dokonuje wyboru trasy między stacją źródłową a docelową, wzdłuż której przesyłane są pakiety. Odpowiada też za ochronę sieci przed przeciążeniami, w tym - przed powstaniem zakleszczeń w węzłach sieci. W przypadku wzajemnej współpracy sieci komputerowych protokoły tej warstwy są odpowiedzialne za "przeźroczysty" przekaz informacji między sieciami, dokonując w szczególności segmentacji i resegmentacji przesyłanych pakietów. Przeźroczystość przekazu oznacza przy tym brak ingerencji poszczególnych sieci w zawartość przekazywanych pakietów. Warstwa pozwala też na multipleksację połączeń sieciowych oraz wykrywanie i korekcję błędów w celu zagwarantowania wymaganej jakości przekazu danych. W zależności od jakości oferowanych usług sieciowych definiowane są trzy klasy sieci (A, B i C) z klasą A gwarantującą praktycznie niezawodny przekaz pakietów w trybie połączeniowym oraz klasą C dopuszczającą "gubienie" pakietów (sieć datagramowa).

**Warstwa transportowa** (WT) jest pierwszą warstwą (licząc od warstwy fizycznej) mającą nadzór nad całością połączenia między stacją źródłową i stacją docelową. Ma ona za zadanie zagwarantowanie niezawodnego i "przeźroczystego" przekazu danych między stacjami końcowymi. W zależności od typu podsieci komunikacyjnej i jakości oferowanych przez nią usług protokoły transportowe mogą sterować przepływem (ang. *flow control*) wykorzystując, podobnie jak w warstwie łączącej danych, mechanizmy okienkowe oraz realizować wykrywanie błędnych bądź straconych pakietów, gwarantując tym samym integralność przesyłanych wiadomości. W zależności od możliwości oferowanych przez oprogramowanie warstwy transportowej, w zakresie wykrywania błędów przy przekazie informacji, definiuje się 5 klas protokołów transportowych

- prosty protokół klasy 0 (TP0) - bez mechanizmów protekcji, zalecany do stosowania w sieciach klasy A;
- protokół klasy 1 (TP1) realizujący podstawowe funkcje wykrywania błędów - zalecany do wykorzystania w sieciach klasy A lub B;
- protokół klasy 2 (TP2) - dopuszczający multipleksowanie wielu połączeń transportowych w jednym połączeniu sieciowym i realizujący niezależne sterowanie przepływem informacji dla każdego połączenia transportowego;
- protokół klasy 3 (TP3) oferujący multipleksowanie połączeń i przywracanie prawidłowej pracy (resynchronizacja) sieci w przypadku wystąpienia niesprawności - zalecany dla sieci typu B;
- protokół klasy 4 (TP4) z pełnym zestawem funkcji wykrywania błędów i przywracania prawidłowej pracy sieci w przypadku wykrycia niesprawności - zalecany dla sieci datagramowych, tj. klasy C.

Głównym zadaniem warstwy transportowej w modelu ISO-OSI jest zagwarantowanie niezawodnej wymiany informacji między dwoma użytkownikami końcowymi. Uwzględnia to zarówno wykrywanie jak i retransmisję wszystkich błędnie przesyłanych lub straconych bloków danych. Jednocześnie warstwa WT dostarcza usług transportowych warstwie sesji.

W przypadku realizacji usług transportowych typu połączeniowego konieczne jest zestawienie połączenia, inicjowane po odbiorze z warstwy sesji odpowiedniego polecenia. Dokonywana jest wówczas negocjacja warunków przekazu danych i wybór klasy protokołu. Tworzona jest też ścieżka dupleksowa, zapewniająca dwukierunkową normalną wymianę informacji między parą procesów aplikacyjnych.

Protokoły transportowe klasy 2 i 4 (TP2 i TP4) pozwalają również na szybki przekaz krótkich bloków danych, szczególnie przydatny w stanach blokady lub przeciążenia sieci.

W celu ograniczenia rozprzestrzeniania się stanu przeciążenia sieci, protokół transportowy TP4 ma wbudowany mechanizm modyfikacji szerokości okna, pozwalający na modyfikację dopuszczalnej liczby pakietów przesyłanych bez potwierdzenia. Szerokość okna w stanach przeciążenia węzłów sieci ograniczona jest do 1, co oznacza konieczność potwierdzania każdego przesłanego pakietu.

Warstwa transportowa może też dokonywać podziału zbyt długich wiadomości na segmenty numerowane kolejnymi liczbami modulo N.

W przypadku multipleksowania połączeń transportowych w jednym połączeniu sieciowym, każdemu z połączeń transportowych przyporządkowany jest unikatowy numer 16-bitowy.

**Warstwa sesji** (WS) zapewnia środki do nawiązywania i rozwijywania sesji oraz zarządzania połączeniem (sesją) pomiędzy dwoma procesami. W tym celu protokół sesji może:

- realizować kontrolę połączenia poprzez tzw. punkty synchronizacji,
- dokonywać zawieszenia oraz restartu połączenia.

Ponadto warstwa sesji steruje dialogiem między procesami, określając kto (który z komunikujących się procesów), kiedy i jak długo może przesyłać informacje.

**Warstwa prezentacji** (WP) zapewnia przekształcanie danych użytkownika do postaci standardowej stosowanej w sieci. Warstwa ta realizuje też utajnianie przesyłanych informacji, dokonując szyfrowania lub wprowadzając zabezpieczenia kryptograficzne. Zapewnia też kompresję danych oraz dokonuje stosownej konwersji formatów i typów danych.

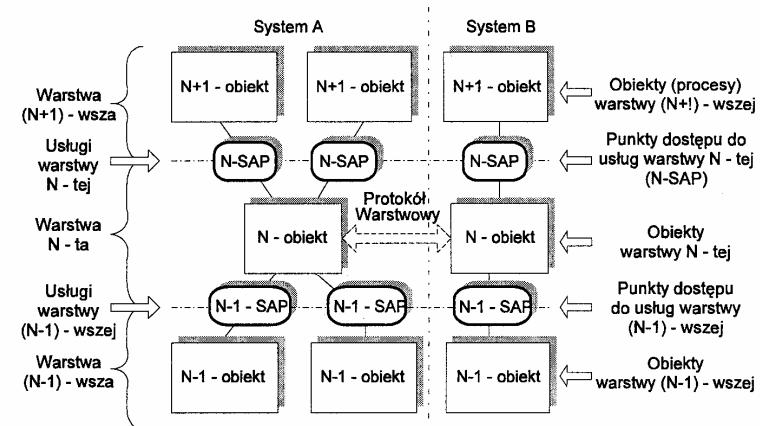
**Warstwa zastosowań (aplikacji)** (WA) zapewnia obsługę użytkownika w dosięgu do usług oferowanych przez środowisko OSI. W szczególności oprogramowanie tej warstwy pozwala na:

- transmisję plików oraz działanie na zdalnych plikach,
- dostęp i działanie na zdalnych bazach danych,
- pracę procesu użytkownika jako terminala zdalnego komputera,
- zarządzanie transmisją i wykonywaniem zdalnych zadań obliczeniowych,
- rozsyłanie poczty elektronicznej.

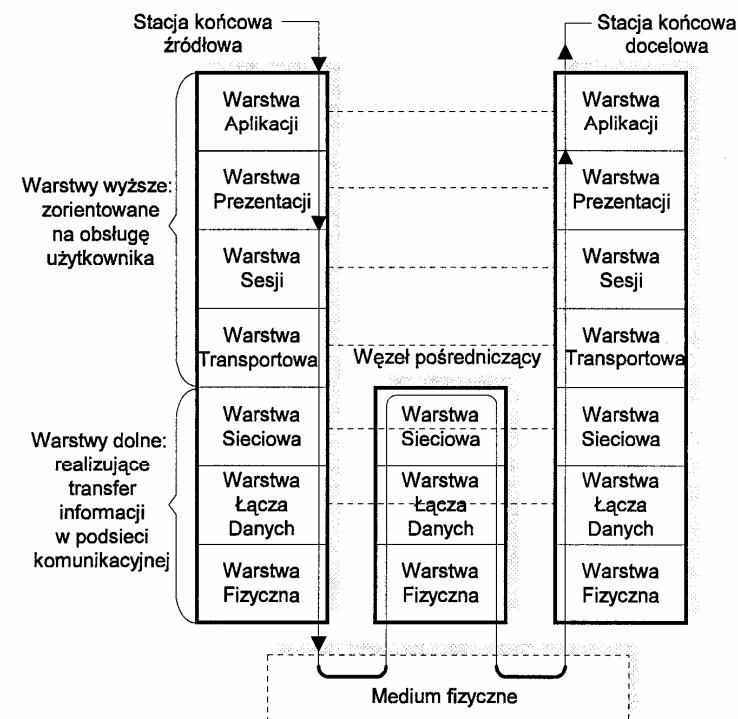
**Liczby warstw, ich nazwy oraz, częściowo, realizowane przez nie funkcje mogą różnić się w różnych warstwowych architekturach sieciowych** (por. rysunek 1.4). W każdej z tych architektur koncepcja współpracy warstw jest jednakże taka sama. Zadaniem warstwy  $N$ -tej jest oferowanie usług transportowych (ang. *transport services*) warstwie wyższej tj.  $N+1$ -wszej, z jednoczesnym zagwarantowaniem izolowania warstwy  $N+1$ -wszej od sposobu realizacji tych usług. Zbiór zasad i konwencji stosowanych przy wymianie informacji między obiekttami (ang. *entities*)/procesami warstwy  $N$ -tej w komunikujących się stacjach (węzłach sieci) nazywamy umownie protokołem warstwy  $N$ -tej. Obiekty tej samej warstwy, w różnych komputerach, realizując tzw. komunikację warstwową, nawiązując warstwowe połączenie logiczne (por. rysunek 1.5a). W rzeczywistości dane nie są jednakże przesyłane bezpośrednio między tymi obiekttami. Przepływ danych odbywa się za pośrednictwem warstw niższych - połączonych wzajemnie interfejsami (stykami, punktami dostępu do usług) programowymi (lub sprzętowymi) - i medium fizycznego, zgodnie z zasadą pokazaną na rysunku 1.5b. Linie przerywane ilustrują istnienie komunikacji logicznej między warstwami.

Warstwa	ISO	SNA	DNA	TCP/IP
7	Aplikacji	Usług transakcyjnych	Użytkownika	
			Zarządzania	
6	Prezentacji	Usług prezentacji	Aplikacji	Aplikacji
5	Sesji	Synchronizacji przepływu	Nadzoru nad sesją	
		Sterowania transmisją danych		
4	Transportowa		Transportowa	Transportowa TCP/UDP
3	Sieciowa	Nadzoru nad ścieżką połączeniową	Sieciowa / routingu	Międzysieciowa IP/ICMP
2	Łącza danych	Sterowania łączem danych	Łącza danych	Dostępu do sieci
1	Fizyczna	Fizyczna	Fizyczna	Fizyczna

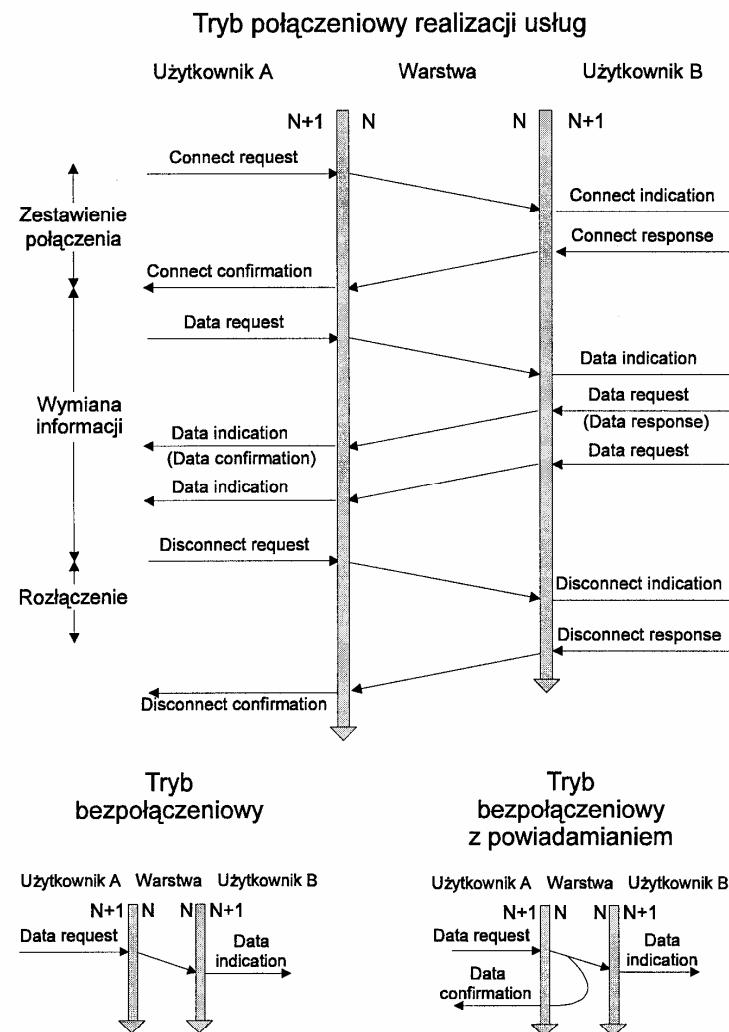
Rys. 1.4. Porównanie wybranych warstwowych architektur sieciowych



Rys. 1.5a. Ilustracja współpracy warstwowej



Rys. 1.5 b. Ilustracja przepływu danych za pośrednictwem warstw niższych



Rys. 1.6. Ilustracja trybów wymiany informacji między obiektami tej samej warstwy

**Programowe styki międzywarstwowe definiują, w modelu ISO-OSI, oferowane usługi oraz operacje podstawowe (ang. primitives) wymieniane między warstwami**, a wymagane do właściwego sterowania przepływem informacji i "egzekwowania" realizacji usług. Wymiana informacji między obiektami warstwy N-tej może odbywać się w jednym z dwóch podstawowych trybów pracy: trybie

### 1.3.2 Architektura SNA

połączeniowym (ang. *connection - oriented service*) lub trybie bezpołączeniowym (ang. *connectionless service*). W zależności od rodzaju usługi realizowane są pewne typowe sekwencje operacji podstawowych. Przykłady takich operacji ilustruje rysunek 1.6. Tryb połączeniowy porównywany jest przy tym do typowego połączenia telefonicznego, w którym wyróżniamy trzy fazy: zestawianie połączenia, wymianę informacji i rozłączenie. Z kolei tryb bezpołączeniowy ma swoją analogię w systemie pocztowym. Możemy przy tym mówić o różnych jego wersjach. Wersji niepewnej/zawodowej (ang. *unreliable* - por. korespondencja zwykła) lub wersji pewnej/niezawodnej uwzględniającej przesyłanie powiadomień (ang. *reliable* lub *connectionless acknowledged service* - por. korespondencja polecona).

Do opisu usług świadczonych przez warstwę WŁD oraz wybranych zasad współpracy międzywarstwowej powrócimy w rozdziale 2, dokonując ogólnej charakterystyki pracy warstwy łączącej danych. Problematyka typów usług świadczonych w sieciach będzie też przedmiotem rozoważań w rozdziale 4, przy okazji omawiania lokalnych sieci komputerowych.

Czytelnika zainteresowanego powyższą tematyką, tj. zagadnieniami usług, sposobami ich realizacji oraz zasadami obowiązującymi przy współpracy międzywarstwowej i warstwowej odsyłamy również do bogatej literatury w języku polskim lub angielskim zawartej w załączonej bibliografii.

### 1.3.2 Architektura SNA

**Architektura SNA** (ang. *Systems Network Architecture*) jest popularnym modelem warstwowy o dominującym znaczeniu w USA. Model ten w swojej pierwotnej postaci **został opracowany w 1974 r. w celu zapewnienia możliwości współpracy różnych typów terminali i komputerów produkowanych przez firmę IBM**. Architektura ta ogranicza więc w sposób naturalny dostęp użytkowników dysponujących sprzętem innym niż firmy IBM do zasobów sieciowych SNA.

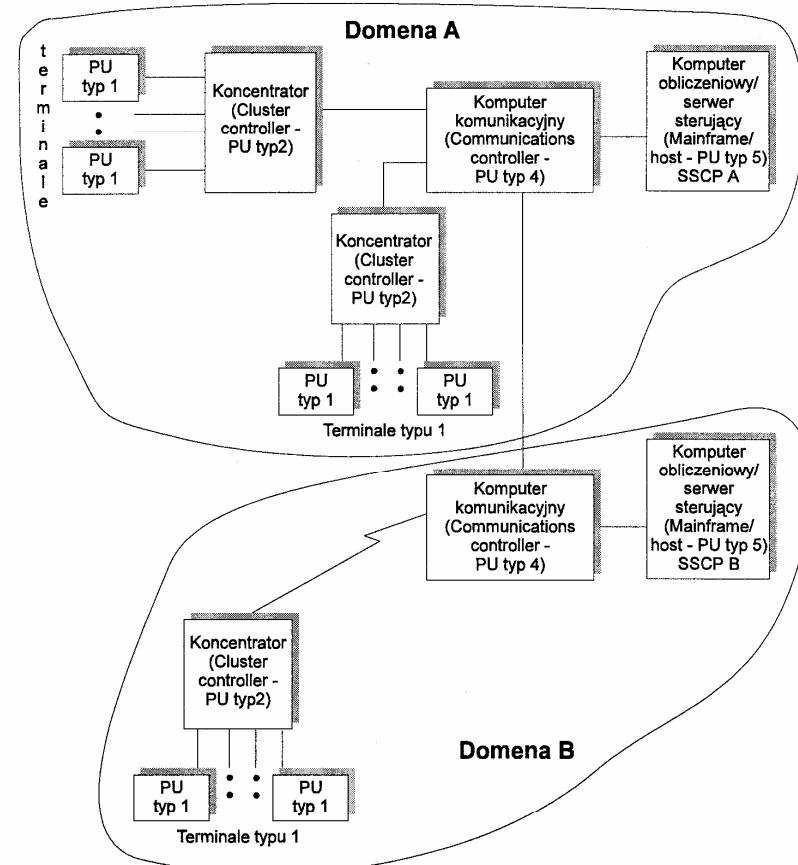
Struktura sieci SNA jest hierarchiczna z wydzieleniem kilku warstw czy też typów urządzeń funkcjonalnych. Urządzenia końcowe, tworzące warstwę najwyższą, dołączane są do sieci za pośrednictwem specjalizowanych koncentratorów, nazywanych kontrolerami (ang. *cluster controller*) i tworzących warstwę drugą. Kolejną warstwę sprzętową stanowią komputery komunikacyjne (ang. *communication controllers*). Jak w większości struktur hierarchicznych zarządzanie podsiecią jest skoncentrowane. Sterowanie procesami nawiązywania połączeń między stacjami sieci SNA realizowane jest (z pewnymi wyjątkami) przez centralne komputery (ang. *host computers - mainframes*) - spełniające rolę swoistych serwerów zarządzających, wyposażonych w pakiety oprogramowania SSCP (ang. *System Service Control Program*). Struktura pojedynczego fragmentu sieci - domeny - jest więc drzewiasta. Należy tu zwrócić uwagę na duże podobieństwo organizacji pracy sieci SNA do rozwiązań implementowanych

w sieciowych systemach operacyjnych (ang. NOS - *Network Operating Systems*) dla sieci LAN - realizujących model "klient-serwer".

Przed opracowaniem architektury SNA, do komunikowania się produktów firmy IBM stosowano kilkadziesiąt różnych metod dostępu i protokołów sterowania połączeniami. Pierwsza struktura sieci z architekturą SNA miała tylko jeden komputer zarządzający. Była to więc duża pojedyncza domena. Kolejne wersje modelu SNA dodawały nowe protokoły komunikacyjne i nowe aplikacje sieciowe. Wersja 2, pochodząca z 1976 roku znacznie uproszczała zarządzanie procesami komunikacyjnymi. Wersja ta dopuszczała stosowanie dwóch protokołów, a mianowicie BSC i SDLC do sterowania połączeniem logicznym między węzłami - jednakże bez możliwości wspólnego wykorzystania pojedynczego łącza przez terminale stosujące protokoły BSC i SDLC. Dokonano też podziału sieci na wiele podzbiorów (domen). W każdym z nich umieszczono komputer komunikacyjny (ang. *communication controller*), zadaniem którego było (i nadal jest) zapewnianie zdalnego dostępu do programów i baz danych danej domeny, oraz sterowanie połączeniem użytkownika z innym obszarem sieci. Połączenia z innymi obszarami sieci (z komputerami zarządzającymi w innych domenach) dokonywane są przy tym w sieciach SNA z użyciem specjalnych protokołów dostępu VTAM (ang. *Virtual Telecommunications Access Method*) i pakietów NCP (ang. *Network Control Program*).

Strukturę sieci SNA z uwzględnieniem czterech warstw urządzeń funkcjonalnych pokazuje rysunek 1.7. Rozbudowa sieci SNA do postaci wielodomenowej spowodowała też pewne utrudnienia w dołączaniu nowych urządzeń do sieci. Sieć SNA jest bowiem siecią w znacznej mierze statyczną, w której dodawanie lub usuwanie urządzeń końcowych wymaga modyfikacji tablic adresowych w oprogramowaniu SSCP komputerów zarządzających. Zmiany te są związane z koniecznością generacji i modyfikacji makroinstrukcji w oprogramowaniu NCP komputerów komunikacyjnych oraz oprogramowaniu komunikacyjnym VTAM komputerów zarządzających. Pakiety SSCP są przy tym elementami oprogramowania VTAM. Moduły SSCP poza tablicami adresowymi urządzeń sieci zawierają też tablice routingu i tablice translacji używane przy zestawianiu połączeń i sterowaniu przepływem informacji. Kolejne wersje modelu SNA rozszerzyły nieco możliwości sieci w zakresie zarządzania jej konfiguracją. Wprowadzenie pakietu oprogramowania CMC (ang. *Communications Management Configuration*) zarządzającego strukturą topologiczną sieci umożliwiło komputerowi komunikacyjnemu szybsze podejmowanie decyzji o konieczności rekonfiguracji strukturalnej oraz wyborze alternatywnych tras przepływu informacji. Wersja 5 z 1984 roku rozszerzyła możliwości adresowania ramek SDLC oraz wpłynęła istotnie na ułatwienie wzajemnych połączeń pomiędzy odrębnymi sieciami SNA. Dodatkowo wersja ta dopuściła bezpośrednią komunikację warstwową typu peer-to-peer pomiędzy wybranymi obiekttami (urządzeniami końcowymi) sieci, tj. z pominięciem komputera zarządzającego, upodabniając tym samym zasady realizacji połączeń do opisanych w modelu ISO-OSI. Możliwość

taką posiadają jednostki fizyczne PU 2.1 (ang. PU - *Physical Unit*) korzystające z programu APPC (ang. *Advanced Program-to-Program Communications*). Kolejne modyfikacje architektury SNA wzbogaciły też istotnie zakres usług oferowanych przez sieci IBM - SNA.



Rys. 1.7. Przykład sieci SNA z dwiema domenami: PU oznacza urządzenie sieci SNA nazywane też adresowlaną jednostką fizyczną (ang. *physical unit*)

Opracowany przez IBM **model SNA definiuje 7 warstw**; zgodnie z ilustracją pokazaną na rysunku 1.4. W modelu tym dokonano rozdziału funkcji związanych z działaniem podsieci komunikacyjnej i przesyaniem ciągów bitów (warstwy 1-3) od ogólnych zadań sterowania przekazem informacji (warstwy 4-6) w postaci generowanej/odbieranej przez użytkownika.

Dokonując porównania funkcji realizowanych przez warstwy modelu SNA z funkcjami modelu ISO-OSI zauważamy, że najistotniejsza różnica dotyczy odmiennego niż w OSI sposobu organizacji warstw 3-5. W szczególności:

- zestawy funkcji warstwy sieciowej i transportowej modelu OSI tworzą warstwę 3 - Nadzoru nad Ścieżką Połączeniową (ang. *Path Control*),
- zestaw funkcji warstwy sesji modelu OSI został z kolei podzielony na dwie warstwy modelu SNA: Synchronizacji Transmisji (ang. *Data Flow Control*) i Sterowania Transmisją (ang. *Transmission Control*).

Powyższe sformułowania mają oczywiście charakter dość luźnej oceny obu modeli.

Przejdziemy obecnie do krótkiej prezentacji podstawowych funkcji warstw SNA.

Podobnie jak w architekturze OSI zaprezentujemy przykładowe zadania warstw poczynając od warstwy fizycznej.

**Warstwa fizyczna** (ang. *Physical Control*) jest odpowiedzialna za transmisję bitów poprzez łącze fizyczne. Definiuje ona styl sprzętowy pomiędzy zakończeniem użytkownika DTE (ang. *Data Terminal Equipment*), a zakończeniem sieciowym DCE (ang. *Data Circuit - Terminating Equipment*). Styk ten opisywany jest charakterystykami: mechaniczną, elektryczną, funkcjonalną i proceduralną. Najpopularniejsze standardowe rozwiązania tej warstwy to styk RS-232 oraz podwarstwa fizyczna standardu IEEE 802.5.

**Warstwa sterowania łączem danych** (ang. *Data Link Control*) ma za zadanie sterowanie przepływem ramek między sąsiednimi węzłami sieci. Inicjuje ona i rozwiązuje połączenia logiczne. Warstwa ta wprowadza zabezpieczenia kodowe, wykrywa błędy i podejmuje decyzje o retransmisji. W SNA funkcjonowanie tej warstwy wiąże się przede wszystkim ze standardowymi protokołami SDLC, BSC oraz Token Ring (IEEE 802.5).

**Warstwa nadzoru nad ścieżką połączeniową** (ang. *Path Control*) zajmuje się sterowaniem przepływem danych między węzłami sieci. Na podstawie adresu stacji docelowej ustalana jest optymalna (nie zawsze najkrótsza) trasa połączenia. Warstwa ta oferuje przy tym selekcję dróg pierwszego i drugiego wyboru i tworzenie ścieżek wirtualnych lub routing wielodrogowy. Do zadań tej warstwy należy również zapobieganie zalewaniu stacji docelowej nadmiarem pakietów (ang. *flow control*) generowanych przez stację źródłową. Innymi zadaniami tej warstwy są określanie klasy świadczonych usług oraz zapewnianie segmentacji/resegmentacji wiadomości.

**Warstwa sterowania transmisją danych** (ang. *Transmission Control*) śledzi zmiany stanów połączenia (sesji) między użytkownikami (określa czy połączenie trwa, czy kolejne jednostki danych napływają, i czy są wysyłane we właściwej kolejności). Warstwa ta dzieli połączenie (sesję) na pewne segmenty. Jeżeli przewidziane jest utajnianie przesyłanej wiadomości, to dokonuje ona stosownych zabezpieczeń.

**Warstwa synchronizacji przepływu** (ang. *Data Flow Control*) jest odpowiedzialna za synchroniczny przepływ danych podczas sesji. Grupuje ona dane w logiczne jednostki, określa prawo do nadawania i odbioru danych (szczególnie istotne przy dwukierunkowym przepływie danych). Warstwa ta odpowiada też za wykrywanie ewentualnych błędów warstw wyższych.

**Warstwa usług prezentacji** (ang. *Presentation Services*) przygotowuje dane kierowane od/do użytkownika we właściwym alfabetie i formacie - pozwalając tym samym na ich prawidłową prezentację na ekranie monitora.

**Warstwa usług transakcyjnych/aplikacji** (ang. *Transaction Services/Application*) obejmuje wszystkie aplikacje udostępniane użytkownikom sieci. Dotyczy to w szczególności przekazu i wymiany dokumentów oraz dostępu do zasobów sieciowych.

Podstawowe elementy architektury SNA stanowią przy tym trzy programy i protokoły, sterujące przepływem informacji w sieci SNA. Są to:

- Pakiety oprogramowania komunikacyjnego VTAM (ang. *Virtual Telecommunications Access Method*) - rezydujące w komputerach głównych poszczególnych domen, nadzorujące sesje pomiędzy programami aplikacyjnymi, terminalami i stacjami roboczymi. Pakiety VTAM zawierają też oprogramowanie SSCP (ang. *System Service Control Point*) zapewniające centralne zarządzanie jednostkami fizycznymi i logicznymi danej domeny. Oprogramowanie VTAM stanowi styk pomiędzy aplikacjami komputera głównego a podsiecią komunikacyjną, pełniąc w tym zakresie funkcje zbliżone do funkcji realizowanych przez warstwy sesji i prezentacji w modelu OSI.
- Oprogramowanie sterujące połączeniem - NCP (ang. *Network Control Program*) - zainstalowane w komputerach komunikacyjnych i odpowiedzialne za wybór trasy oraz nadzór nad połączeniem transportowym w sieci SNA. Przyjmuje się zwykle, że pakiet NCP pełni zadania przypisywane warstwom sieciowej i transportowej modelu ISO-OSI.
- Ostatnim, istotnym, elementem architektury SNA jest protokół SDLC opisany w rozdziale 3.4. Jest on wykorzystywany do sterowania połączeniami pomiędzy urządzeniami przyłączonymi do sieci SNA. Protokół SDLC realizuje zestaw funkcji przypisanych warstwie łączu danych.

W sieci SNA z każdym jej urządzeniem wiąże się pojęcie jednostki fizycznej PU (ang. *Physical Unit*). Nazwa ta nie odnosi się przy tym do układu fizycznego, jako takiego, lecz do zespołu elementów, który to zespół zapewnia możliwość nadzoru i sterowania pracą terminala, kontrolera, procesora czy też łączu w sieci SNA. W układach programowalnych, takich jak komputery główne-zarządzające, czy też komputery komunikacyjne, jednostka PU jest implementowana programowo. W monitorach lub niektórych kontrolerach może być to ROM. W sieci SNA każda jednostka działa pod nadzorem programu zarządzającego

<sup>3</sup> — Sieci LAN, MAN i WAN

SSCP komputera głównego domeny. Typy jednostek PU wykorzystywanych do tworzenia sieci SNA podane są w tabeli 1.1. W SNA definiuje się też jednostki logiczne LU (ang. *Logical Unit*). LU jest z kolei interfejsem - elementem stylistycznym pomiędzy użytkownikiem końcowym, a siecią SNA. Poprzez LU użytkownik uzyskuje dostęp do zasobów sieciowych oraz możliwość nadawania i odbioru informacji przesyłanych poprzez sieć. Każda jednostka PU może mieć jedną lub więcej jednostek typu LU. W sieci SNA wszystkie jednostki PU oraz LU mają unikatowe adresy. Jednostką adresowalną jest też oprogramowanie zarządzające SSCP.

Architektura SNA umożliwiała pierwotnie użytkownikom sieci zestawianie połączeń jedynie z programami aplikacyjnymi komputerów głównych. Można zatem było mówić o całkowicie hierarchicznej architekturze SNA. Po zestawieniu sesji oprogramowanie NCP komputera komunikacyjnego sterowało przepływem informacji pomiędzy użytkownikiem i aplikacją. Ze wzrostem możliwości dokonywania obliczeń przez same urządzenia końcowe pojawiła się potrzeba realizacji sesji pomiędzy komputerami osobistymi, z pominięciem komputera głównego. Spowodowało to pewne modyfikacje w architekturze SNA pozwalające na realizację komunikacji warstwowej (typu peer-to-peer). W tym celu IBM zdefiniował jednostkę fizyczną PU 2.1, która w przypadku zastosowania jednostki logicznej LU 6.2 i zaimplementowania oprogramowania APPC (ang. *Advanced Program-to-Program Communications* - jest to właściwie nazwa handlowa protokołu LU 6.2), może nawiązać sesję z inną jednostką PU 2.1 bez pośrednictwa komputera głównego.

Tabela 1.1. Typy urządzeń w sieci SNA

Typy PU	Funkcje urządzenia	Oznaczenie sprzętu IBM
PU-Typ5	Komputer obliczeniowy/serwer sterujący (Mainframe)	S/370, 43XX, 308X
PU-Typ4	Komputer komunikacyjny (Communications controller)	3705, 3725, 3745
PU-Typ3	obecnie nie zdefiniowany	
PU-Typ2.1	Komputer z zaimplementowanym protokołem APPN (jednostka logiczna LU6.2)	dowolny komputer
PU-Typ2	Koncentrator (Cluster controller)	3174, 3274, 3276
PU-Typ1	Terminal (urządzenie końcowe)	3180, PC z adapterem SNA

W roku 1985 IBM wprowadził architekturę APPN (ang. *Advanced-Peer-to-Peer Networking*) integrując ją z SNA. APPN przenosi część usług realizowanych w komputerach głównych (*mainframe*) do komputerów współpracujących na zasadzie peer-to-peer. Takie rozwiązanie stało się możliwe po przyjęciu założenia, że każdy z komputerów pracujących w sieci jest w stanie samodzielnie

realizować routing oraz zarządzać sesją. Koncepcja komunikacji warstwowej APPN zaczyna odgrywać w SNA coraz istotniejszą rolę.

Nowa wersja oprogramowania komunikacyjnego VTAM komputerów głównych (VTAM wersja 4.1 z 1992 roku) pozwala również tym węzłom na nawiązywanie połączeń (nawiązywanie sesji) z innymi węzłami sieci zgodnie z zasadami komunikacji warstwowej.

W chwili obecnej w SNA definiowane są cztery typy sesji: SSCP-PU, SSCP-LU, SSCP-SSCP oraz LU-LU. Dwa pierwsze rodzaje sesji są realizowane w przypadku żądania lub wymiany informacji diagnostycznych. Trzeci typ pozwala na wymianę informacji pomiędzy programami zarządzającymi SSCP komputerów zarządzających (głównych). Typ ostatni, tj. LU-LU, jest podstawowym rodzajem sesji w SNA. W przypadku nawiązywania sesji między jednostkami logicznymi jedna z nich, nazywana główną (ang. *Primary LU* - PLU), przejmuje na siebie funkcje kontrolne (wykrywanie błędów w transmisji). Druga z zaangażowanych jednostek LU pełni rolę jednostki podległej (ang. *Secondary LU* - SLU). Połączenie jest inicjowane przez jednostkę PLU.

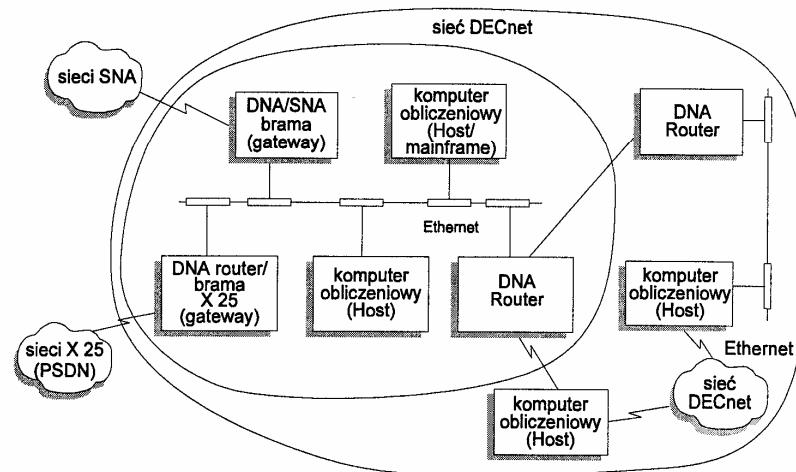
**Architektura SNA zapewnia wewnętrznie sieciową kompatybilność sprzętu IBM.** Jest to o tyle ważne, że na rynku amerykańskim zarówno sprzęt IBM jak i sama sieć SNA odgrywają znaczenie dominujące. Ważną zaletą sieci SNA jest też dość wysoka efektywność zarządzania siecią - między innymi dzięki zaimplementowanym w komputerach komunikacyjnych pakietom oprogramowania NCP, CMC oraz oprogramowaniu NPDA (ang. *Network Problem Determination Application*) pozwalającemu na zbieranie danych statystycznych o stanie kanałów, urządzeń końcowych i modemów. SNA oferuje użytkownikom sieci dużą liczbę aplikacji, szczególnie przydatnych przy automatyzacji prac biurowych.

Jednocześnie SNA wykazuje szereg istotnych wad. Nie pozwala bowiem na pełną integrację podsieci LAN. Jest też architekturą "zamkniętą" - nie definiującą zasad współpracy z innymi systemami sieciowymi. Ponadto SNA nie oferuje ani dynamicznego routingu ani też możliwości dynamicznego przywracania sprawności sieci w przypadku wykrycia uszkodzeń.

### 1.3.3 Architektura DNA

Omawiana w poprzednim paragrafie architektura SNA opracowana została dla zapewnienia wzajemnej komunikacji różnych, częściowo niekompatybilnych urządzeń firmy IBM. **Architekturę warstwową DNA** (ang. *Digital Network Architecture*) zaprojektowano z kolei z myślą o zapewnieniu współpracy sprzętu firmy DEC (ang. *Digital Equipment Corporation*). Dokumentacja modelu DNA obejmuje opisy usług i funkcji poszczególnych warstw oraz realizowanych przez nie protokołów. Sieć DECnet, implemetsująca DNA, obejmuje szereg urządzeń. Należą do nich zarówno routery, będące węzłami tranzytowymi podsieci komunikacyjnej jak też systemy komputerowe VAX różnych typów. **DECnet jest przykładem sieci WAN pozwalającej na integrację odległych sieci LAN.** Do-

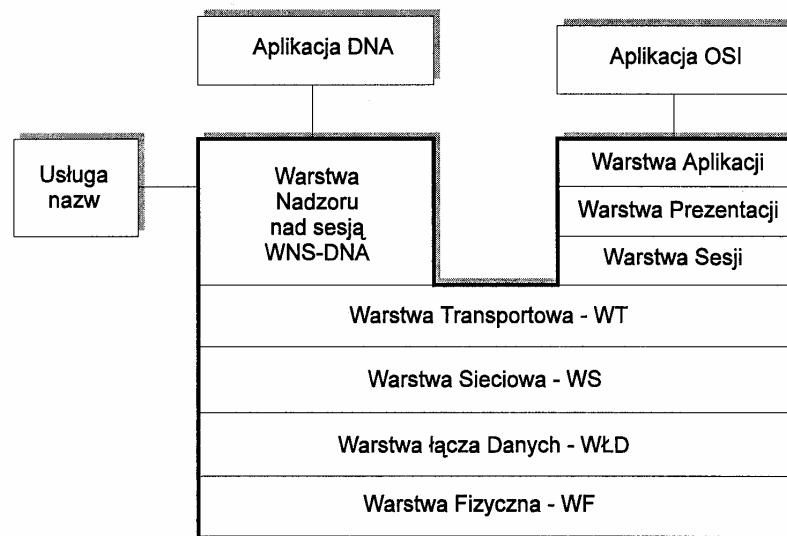
tyczy to w szczególności sieci Ethernet. W tym zakresie firmy DEC, XEROX i Intel podjęły scisłą współpracę. Fragmenty sieci DECnet tworzą przy tym obszary administracyjne nazywane często (podobnie jak w SNA) domenami. Przykładową strukturę sieci DECnet ilustruje rysunek 1.8.



Rys. 1.8. Przykład sieci DECnet

Pierwsza wersja architektury DNA została opracowana w połowie lat siedemdziesiątych; w 1974 roku została zaimplementowana tzw. faza I modelu. Na przestrzeni 20 lat model DNA podlegał znacznym przeobrażeniom. Celem tych zmian, począwszy od początku lat osiemdziesiątych, było zapewnienie jak najpełniejszej zgodności z modelem ISO-OSI. W DNA uwzględniono też potrzeby współpracy sieci DECnet z sieciami o innych architekturach. W fazie III DNA przewidziano np. standardowe pakiety oprogramowania dla routerów i konwerterów protokołów, czy też bram bądź śluз (ang. gateways) pozwalające na współpracę z siecią pakietową X25 oraz sieciami SNA.

W 1987 roku została opracowana wersja DNA, nazywana fazą V. Jej implementację zainicjowano w 1991 roku. **Ten kolejny model DNA zbliża tę architekturę do pełnej zgodności z modelem OSI.** Jak pokazano na rysunku 1.9 model architektury DNA dla fazy V wykazuje przy tym pewną dwoistość: pełną zgodność oferowanych usług, realizowanych funkcji i implementowanych protokołów komunikacyjnych w zakresie warstw od fizycznej do transportowej oraz rozdelenie modelu DNA na dwa strumienie DNA i OSI w zakresie warstw wyższych. Oznacza to, że powyżej warstwy transportowej użytkownik sieci DECnet może korzystać zarówno z protokołów firmowych jak też standardowych protokołów ISO. Należy też zwrócić uwagę na to, że wersja V DNA przewiduje także możliwość współpracy z sieciami TCP/IP.



Rys. 1.9. Architektura warstwowa DNA dla fazy V

Dokonamy obecnie krótkiej prezentacji wybranych cech charakterystycznych poszczególnych warstw modelu DNA.

#### Warstwa fizyczna

Warstwa ta jest w DNA analogiczna do warstwy fizycznej modelu OSI. Specyfikuje ona w szczególności elementy stykowe dla trzech podstawowych typów łączys fizycznych:

- styl RS232 dla połączeń modemowych z wykorzystaniem łączys analogowych;
- układy warstwy fizycznej dla sieci LAN CSMA/CD, tj. standardy IEEE 802.3 i ISO 8802-3 oraz rozwiązanie styku fizycznego dla sieci typu Ethernet;
- układy stykowe sieci FDDI opisane standardami ANSI X3T9.5 i ISO 9314.

#### Warstwa łącza danych

Funkcje i usługi definiowane przez tę warstwę są identyczne jak w modelu OSI. Warstwa WŁD w DNA obejmuje specyfikacje pięciu standardowych protokołów. Są to:

- HDLC (ang. *High level Data Link Control*) - protokół ten definiowany jest przez dokumenty ISO 3009, 4335, 7809 i 8885;

- LAPB (ang. *Link Access Procedure Balanced*) - specyfikacja definiuje podzbior HDLC wykorzystywany w zaleceniu CCITT X25 (również ISO 7776);
- CSMA/CD LAN oraz LAN Ethernet - specyfikacja obejmuje standarde rozwiązań sieci LAN IEEE 802.3 oraz ISO 8802-3, a ponadto wersję 2 specyfikacji Ethernet;
- FDDI - specyfikacja obejmuje część standardów ANSI X3T9.5 (oraz ISO 9314) odpowiadającą WLD;
- DDCMP (ang. *Digital Data Communication Message Protocol*) - protokół ten stanowi element architektury DNA z fazy IV (DNA V zapewnia pełną obsługę urządzeń zaimplementowaną fazą IV DNA).

#### **Warstwa sieciowa**

Warstwa ta jest w pełni zgodna z warstwą sieciową OSI. DNA przewiduje realizację podstawowych standardów ISO w zakresie usług i protokołów trybu bezpołączeniowego (ISO 8348, 8473, 9542, 10589) oraz usług i protokołów połączeniowych (ISO 8348, 8878, 8208). W zakresie warstwy sieciowej główny nacisk położony został przez firmę DEC na obsługę dużych sieci oraz zagwarantowanie możliwości dołączania do sieci DECnet urządzeń komputerowych pochodzących od wielu producentów (o różnych systemach operacyjnych), jak też możliwości współpracy podsieci komputerowych różnych organizacji. W tym celu zaakceptowano ISO-wskie standardy adresowe z unikatowymi adresami globalnymi oraz rozproszone algorytmy routingu.

Najważniejszym zadaniem warstwy WS jest, podobnie jak w innych architekturach, podejmowanie decyzji o wyborze możliwej najlepszej trasy przepływu pakietów pomiędzy stacją źródłową a docelową. W przekazie pakietów, w dużych sieciach DECnet, uczestniczą węzły pośrednie, noszące nazwę routerów. Usługi przekazu pakietów wspomagane są zapożyczonym z ISO-OSI systemem unikatowych adresów sieciowych, o długościach do 20 bajtów. Podstawowym protokołem sieciowym DECnetu jest protokół ISO 8473, będący datagramowym protokołem internetowym (IP OSI). Definiuje on strukturę pakietu, zbliżoną do internetowego protokołu IP z architektury TCP/IP. Mechanizmy zaimplementowane w ISO 8473 zapewniają możliwość segmentacji i resegmentacji pakietów, nadzorowanie ich czasu życia oraz unikanie przeciążeń w sieci. Routing w sieci DECnet realizowany jest zgodnie z protokołem ISO 9542. Protokół ten zapewnia informacje niezbędne do podejmowania w routerach i stacjach końcowych (ang. IS-ES - *intermediate/end systems*) decyzji o wyborze trasy. Wymieniane pomiędzy węzłami sieci informacje sterujące (ang. *end system hello*, *end node hello*, *intermediate system hello* oraz *redirect*) uwzględniają:

- dane na temat konfiguracji sieci, tj. informacje o położeniu routerów oraz nowo dołączanych bądź usuwanych węzłach sieci,
- informacje o korzystniejszych trasach przesyłania pakietów.

W celu usprawnienia routingu, w dużych sieciach DECnet, cały ich obszar dzielony jest na domeny administracyjne, które z kolei dzielone są na mniejsze domeny (obszary) routingu. Definiowany jest przy tym dwupoziomowy routing hierarchiczny. Routing w ramach jednego obszaru realizowany jest w sposób jednorodny. Komunikacja pomiędzy poszczególnymi obszarami odbywa się z udziałem routerów (i zasad routingu) 2-go poziomu.

W wersji IV DNA routing wewnętrz domeny odbywał się z użyciem algorytmu dystrybucyjnego typu dystansowo-wektorowego (odległościowo-wektorowego) (ang. *distance-vector*). Zgodnie z tym algorytmem wszystkie węzły wymieniały między sobą okresowo informacje o topologii sieci.

W fazie V DNA, zaprojektowanej pod kątem obsługi sieci danych, algorytm ten zastąpiono metodą stanu łączą (ang. *link-state*). W tym przypadku routery przekazują informacje o stanach ich łączów prowadzących do wszystkich sąsiednich węzłów. Algorytm ten obejmuje procedury aktualizacji stanów łączów, podejmowania decyzji o wyborze trasy najkrótszej (o najmniejszym koszcie), przesyłania pakietów wzdłuż tras najkrótszych oraz odbioru pakietów napływających do routera.

W celu kierowania ruchem pakietów między domenami stosowane są metody routingu statycznego. Do tego celu wykorzystywane są tablice wyboru tras, przechowywane w routerach poziomu drugiego i pozwalające na wybór tras alternatywnych. Przy konstrukcji tablic wyboru tras routery korzystają z procedur zarządzania siecią DECnet.

Jak wspomnieliśmy wcześniej, routing w sieci DECnet realizowany jest z wykorzystaniem adresowych standardów ISO. Adres sieciowy stacji lub routera składa się z ciągu o długości do 20 bajtów. Obejmuje on adres obszaru (do 13 bajtów), identyfikator węzła w danym obszarze (6 bajtów) oraz typ protokołu warstwy transportowej (1 bajt).

#### **Warstwa transportowa**

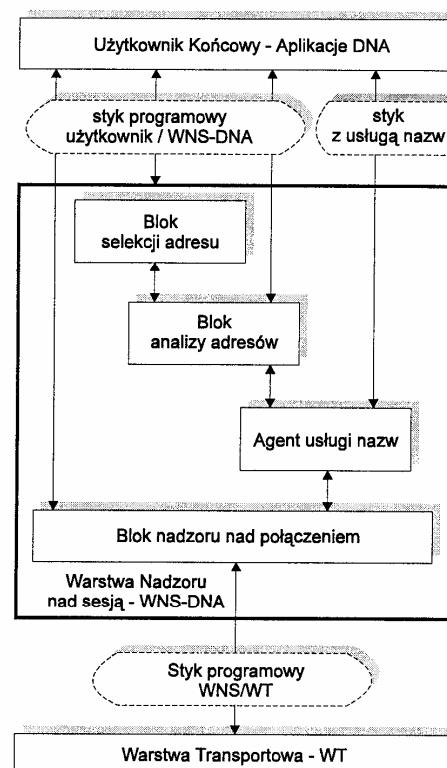
Warstwa ta wspomaga zarówno protokoły transportowe OSI jak też protokół sieci DECnet. W zakresie usług transportowych zgodnych z OSI definiowane są i implementowane klasy 0, 2 i 4, a protokół klasy 4 jest protokołem zalecanym w sieci DECnet. W przypadku realizacji podwarstwy zgodnie z implementacją fazy IV DNA (podwarstwa End-to-End Communication) definiowany jest protokół NSP (ang. *Network Services Protocol*). Warto przy tym zwrócić uwagę na to, że doświadczenia DEC w zakresie NSP posłużyły do opracowania specyfikacji protokołu transportowego OSI klasy 4 (TP4).

Firmowy protokół transportowy sieci DECnet, tj. NSP (ang. *Network Service Protocol*) jest bardziej złożony od protokołów TP ISO. Protokół ten definiuje 14 różnych typów wiadomości przesyłanych poprzez połączenie transportowe. Są to zarówno dane jak też wiadomości sterujące i powiadomienia. Protokół NSP obejmuje przy tym procedury:

- zestawiania połączeń,
- przekazu danych,
- sterowania przepływem,
- unieważniania połączeń,
- rozwiązywania połączeń.

Procedury zestawiania połączenia, jego utrzymania bądź rozwiązywania wykorzystują przy tym dwa niezależne podkanaly, jeden do przesyłania danych normalnych, wymienianych między dwiema jednostkami NSP, drugi natomiast do przesyłania informacji sterujących bądź szybkiego przekazu danych.

#### Warstwy wyższe w architekturze DNA



Rys. 1.10. Organizacja warstwy WNS-DNA

Powyżej warstwy transportowej w architekturze DNA definiowane są dwa zestawy warstw wspomagających dwie klasy aplikacji. Warstwy te mają za

**zadanie integrację oprogramowania sieciowego i komunikacyjnego DNA z systemem operacyjnym oraz oprogramowaniem aplikacyjnym i zarządzającym pracą sieci.** Faza V DNA została zaprojektowana pod kątem wspomagania zarówno aplikacji zgodnych ze standardami ISO jak też aplikacji firmowych DEC. W przypadku zestawu warstw OSI realizowane funkcje, usługi i aplikacje są identyczne jak w opisany wcześniej modelu warstwowym systemu otwartego. W zestawie warstw wspomagającym aplikacje firmowe wyróżnia się Warstwę Nadzoru nad Sesją (WNS-DNA) (ang. Session Control Layer - SCL) oraz aplikacje użytkownika końcowego. Warstwa Nadzoru nad Sesją składa się z kilku bloków funkcjonalnych, których wzajemne relacje ukazuje rysunek 1.10. Są to:

- **Agent Usługi Nazw** - AUN (ang. Naming Service Clerk). Blok ten pozwala na odzyskiwanie atrybutów programów aplikacyjnych - w tym adresów ich lokalizacji w sieci. Programy aplikacyjne (zasoby sieciowe), nazywane obiekty, są identyfikowane w DNA za pomocą nazw. Moduł AUN utrzymuje również informacje o atrybutach lokalnych zasobów stacji.
- **Blok Nadzoru nad Połączeniem** - BNP (ang. Connection Control). Blok ten nadzoruje dostęp do usług warstwy transportowej zarówno w przypadku połączeń pomiędzy aplikacjami sieciowymi, jak też konieczności wymiany informacji między blokami AUN, a serwerami nazw DNA (ang. Naming Servers).
- **Blok Analizy Adresów** - BAA (ang. Address Resolution). Blok BAA zapewnia komunikację z blokiem AUN w celu określenia zbioru protokołów i informacji adresowych przydatnych przy realizacji połączeń między aplikacjami - obiektami: lokalnym i zdalnym.
- **Blok Selekcji Adresu** - BSA (ang. Address Selection). BSA wyznacza protokół i informację adresową, wykorzystywane następnie przy zestawianiu połączenia transportowego.

Ciągle rosnąca złożoność (wielkość) sieci komputerowych narzuca konieczność implementowania efektywnych procedur identyfikacji i lokalizacji stacji użytkowników oraz zasobów sieciowych. Identyfikacja zasobów realizowana jest w DNA za pomocą nazw. Zaimplementowana w DNA usługa nazw udostępnia użytkownikom możliwości jakie daje typowa książka telefoniczna. Użytkownik podaje nazwę pożąданej usługi sieciowej bądź zasobu (obiektu), a otrzymuje zwrotnie zestaw atrybutów związanych z tą usługą (zasobem). Jednym z istotnych atrybutów jest przy tym adres węzła, w którym dany obiekt jest ulokowany. W sieciach DECnet usługa nazw jest rozproszona i zaimplementowana we wzajemnie komunikujących się serwerach nazw. W celu realizacji przekazu wiadomości pomiędzy procesami aplikacyjnymi użytkowników sieci DECnet, realizowanymi zgodnie ze specyfikacją DNA, wiadomość jest każdorazowo przekazywana do warstwy WNS-DNA poprzez interfejs programowy definiowany przez lokalny system operacyjny. Do każdej wiadomości dodawana jest

informacja kontrolna w postaci nagłówka. Tworzona w ten sposób jednostka danych przekazywana jest do warstwy transportowej poprzez odpowiedni punkt dostępu do usług (T-SAP). Architektura DNA definiuje również funkcje pozwalające operatorom i administratorom sieci na planowanie rozbudowy, zarządzanie pracą sieci jak też wypełnianie podstawowych zadań utrzymywaniowych, obejmujących testowanie połączeń, zdalne załadowywanie i usuwanie pakietów oprogramowania.

**Oprogramowanie zarządzające** wydzielone jest w postaci niezależnej platformy (ang. *Network Management Layer*). Zarządzanie globalne siecią DECnet realizowane jest w sposób rozproszony. Całość problematyki zarządzania prezentowana jest w postaci architektury EMA (ang. *Enterprise Management Architecture*) opisującej wzajemne oddziaływanie różnych elementów w sieci, w tym powiązania z poszczególnymi warstwami DNA w węzłach.

**Komunikacja międzywarstwowa w architekturze DNA odbywa się zgodnie z zasadami specyfikowanymi w modelu ISO-OSI.** Do celu tej komunikacji wykorzystywane są prymitywy typu żądanie, powiadomienie, odpowiedź, potwierdzenie (ang. *request, indication, response i acknowledgment*). Z kolei komunikacja logiczna pomiędzy obiektami warstw realizowana jest z wykorzystaniem szeregu protokołów zgodnych ze standardami ISO (w przypadku fazy V) bądź DNA (dla faz od I do IV).

Cechą charakterystyczną i niewątpliwą zaletą sieci DECnet jest zagwarantowanie możliwości komunikowania się jej systemów obliczeniowych z systemami innych sieci. Projektanci architektury DNA opracowali szereg sprzęgów programowych pozwalających na współpracę systemów sieci DECnet z urządzeniami dołączonymi do sieci X25 oraz SNA. W przypadku współpracy DECnet - SNA konieczne jest stosowanie bram (ang. *gateway*) nazywanych też często konwerterami protokołów (ang. *protocol converters*) bądź śluzami. Sieć SNA traktuje urządzenie konwertera jako układ kontrolera (ang. *cluster controller*). W strukturze sieci DNA brama może być przy tym zarówno węzłem sieci rozległej jak też komputerem dołączonym do sieci Ethernet. Faza V DNA przewiduje również współpracę sieci DECnet z sieciami TCP/IP.

### 1.3.4 Architektura TCP/IP

**Celem opracowania zbioru sieciowych protokołów TCP/IP było umożliwienie komunikacji pomiędzy systemami pochodzącyymi od wielu różnych dostawców.**

Zmiany w architekturze TCP/IP są ściśle związane z rozwojem Internetu. Nadzór nad wprowadzaniem stosownych zmian i modyfikacji do sieci sprawuje *Internet Engineering Task Force* (IETF). Zasady działania Internetu ujmują tzw. dokumenty RFC (ang. *Request For Comments*). W latach 1969-1996 opublikowano ponad 1900 takich dokumentów.

Ze względu na ważność TCP/IP dla współdziałania i rozwoju współczesnych sieci komputerowych architekturze TCP/IP poświęcimy w tej książce nieco więcej

miejsc. Po ogólnej prezentacji architektury TCP/IP w niniejszym rozdziale, do omówienia wybranych aspektów, w szczególności nowej wersji protokołu IP (IPv6, IPng), powrócimy w rozdziale 8.

Podstawowe rozwiązania stosowane w rodzinie protokołów TCP/IP są efektem pracy grupy rozwojowej sieci ARPANET, stworzonej w 1968 roku w ramach programu Departamentu Obrony USA. W roku 1971 projekt ARPANET został przejęty przez amerykańską agencję zaawansowanych badań systemów obrony i tam właśnie opracowano protokoły IP (ang. *Internet Protocol*) oraz TCP (ang. *Transmission Control Protocol*). Protokoły TCP/IP są w chwili obecnej najpopularniejszym i najszerzej stosowanym zestawem protokołów wymiany informacji między komputerami. Walnie przyczyniła się do tego publiczna sieć komputerowa Internet skupiająca ponad cztery miliony stacji roboczych.

Warto przy okazji zwrócić uwagę na różne znaczenie przypisywane pojęciu INTERNET:

- internet - pisany z małej litery - jest zbiorem oddzielnich fizycznie sieci, połączonych wspólnym protokołem w jedną sieć logiczną;
- Internet - pisany wielką literą I - jest także zbiorem połączonych sieci, ale na całym świecie, i używających do ich łączenia w jedną sieć logiczną Protokołu Internet IP.

Protokoły Internetu są używane również w środowisku UNIX-owym dla sieci lokalnych, w szczególności protokoły TCP/IP stosowane są do komunikacji w sieciach LAN typu Ethernet.

**TCP/IP powstało dużo wcześniej niż model odniesienia ISO-OSI i dlatego też warstwy nie są tak wyraźnie i jednoznacznie zdefiniowane, a ich obecność (istnienie samej architektury warstwowej) wynika bardziej z analizy funkcji realizowanych przez protokoły, niż z założień projektantów sieci.** Pod koniec lat siedemdziesiątych pojawiła się koncepcja integracji zbioru protokołów TCP/IP z protokołami OSI. Koncepcja ta nie została jednak wdrożona.

W architekturze TCP/IP wyróżnić można siedem warstw, które jednakże niezbyt dokładnie odpowiadają warstwom modelu ISO-OSI (patrz rysunek 1.11).

Porównując warstwy w modelu odniesienia ISO/OSI z architekturą TCP/IP warto zwrócić uwagę na to, że:

- W przypadku warstw 1 i 2 TCP/IP korzysta z już istniejących standardów sieciowych, o różnych technologiach (np. z Ethernetem).
- Za podstawowy protokół warstwy 3 przyjmuje się internetowy protokół IP (ang. *Internet Protocol*), który izoluje warstwy wyższe od zagadnień pracy sieci. Zajmuje się on adresowaniem oraz wymianą danych między niejednorodnymi systemami. Dodatkowo, warstwa 3 używa internetowy protokół sterowania przepływem wiadomości ICMP (ang. *Internet Control Message Protocol*).

- Większość zadań zarządzania i sterowania przepływem wiadomości, które charakteryzują TCP/IP, jest realizowanych na poziomie warstwy transportowej przez protokół TCP. Protokół ten gwarantuje, że dane dostarczane do adresata są dokładnie zgodne z wysyłanymi przez nadawcę. Innym dostępnym, lecz mniej popularnym w użyciu, protokołem tej warstwy jest bezpołączniowy protokół datagramowy UDP (ang. *User Datagram Protocol*). UDP nie gwarantuje jednakże pełnej poprawności i integralności przesyłanych danych. UDP jest przeznaczony do realizacji usług czasu rzeczywistego.
- Warstwie 5 i częściowo 6 odpowiadają protokoły Telnet i wirtualnego terminala, które podtrzymują wirtualne połączenie terminal-komputer główny (ang. *host*) oraz pozwalają na zdalne logowanie się użytkowników.
- Z kolej warstwom 6 i 7 odpowiada protokół przekazu plików FTP (ang. *File Transfer Protocol*), który zabezpiecza przekazywanie plików między niejednorodnymi urządzeniami i systemami operacyjnymi.



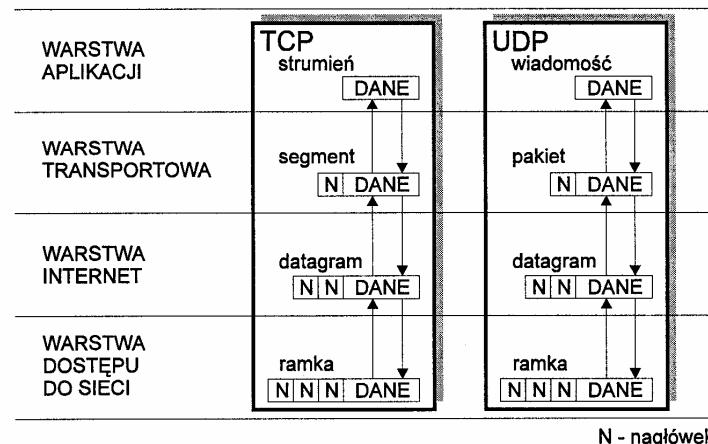
Rys. 1.11. Czterowarstwowy model TCP/IP i jego porównanie z modelem ISO-OSI

Często, model warstwowy TCP/IP przedstawia się za pomocą jedynie czterech warstw (patrz rysunek 1.11). Model ten tworzą wówczas:

- 1) warstwa dostępu do sieci - odpowiadająca w modelu ISO-OSI dwóm pierwszym warstwom tj. warstwie fizycznej i warstwie łącza danych;
- 2) warstwa międzysieciowa Internet - odpowiadająca w modelu ISO-OSI warstwie trzeciej;

- 3) warstwa transportowa - odpowiadająca w modelu ISO-OSI warstwie czwartej;
- 4) warstwa aplikacji - odpowiadająca w modelu ISO-OSI warstwom piątej, szóstej i siódmej.

*Koncepcja funkcjonowania sieci TCP/IP, zarówno w zakresie komunikacji międzywarstwowej, jak też warstwowej, jest taka sama jak w modelu ISO-OSI.* Informacje przepływają w dół "stosu", gdy są wysyłane do sieci, lub w górę, gdy są otrzymywane z sieci. Podeczas przepływu danych od warstwy aplikacji w dół, każda z warstw, do danych otrzymywanych z warstwy wyższej, dodaje własną informację sterującą w postaci nagłówka (ang. *header*). Proces ten nazywany jest enkapsulacją. Po stronie odbiorczej sieci dane są z kolei wydobywane ze struktury ramki i przetwarzane w odwrotnym (w stosunku do poprzedniego) porządku. Każda warstwa traktuje informację przychodząą z warstwy niższej jako nagłówek i część danych. Jedynie dane są przekazywane do warstwy wyższej (patrz rysunek 1.12).

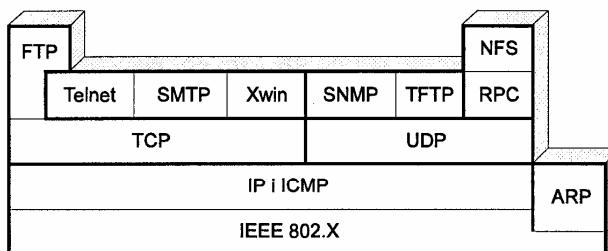


Rys. 1.12. Jednostki danych i ich przepływy w strukturze protokołów TCP/IP (UDP/IP)

Każdej z warstw modelu TCP/IP odpowiadają różne protokoły. Ważniejsze z nich oraz ich umiejscowienie przedstawia rysunek 1.13.

Protokoły warstw 1 i 2 są zależne od technologii sieci składowych Internetu. Protokoły tych warstw, tworzące Warstwę Dostępu do Sieci (ang. *Network Access Layer*), odpowiedzialne są za dostarczanie danych do innych urządzeń bezpośrednio przyłączonych do sieci. W przypadku sieci typu LAN może to być Ethernet lub Token-Ring. Dla sieci typu WAN stosowane są protokoły *Point-to-Point Protocol* (PPP), *Serial Line Internet Protocol* (SLIP), X.25 i Frame Relay. W odróżnieniu od protokołów warstw wyższych, protokoły warstwy dostępu

muszą znać szczegóły sieci fizycznej (jej strukturę, adresowanie, itd.), w celu dopasowania formatu danych do wymogów sieci.



Rys. 1.13. Ważniejsze protokoły w architekturze protokołów TCP/IP

W koncepcji funkcjonowania Internetu szczególne miejsce zajmuje warstwa międzysieciowa, której działanie wiąże się integralnie z protokołem IP. Do funkcji realizowanych przez warstwę międzysieciową należy enkapsulacja IP datagramów w ramki, transmitowane następnie przez sieć oraz odwzorowywanie (ang. *mapping*) adresów IP na fizyczne adresy używane przez sieć. TCP/IP używa własnego schematu adresowania, jednoznacznie identyfikującego każdy komputer w Internecie. Protokół wymiany międzysieciowej, jakim jest IP, realizuje podstawowe usługi dostarczania pakietów, na których opiera się działanie TCP/IP. Protokół IP przenosi dane pomiędzy Warstwą Dostępu do Sieci a Warstwą Transportową. W tym celu definiuje on strukturę pakietu, nazywanego w tym przypadku datagramem. Przeprowadza też, o ile jest to konieczne, fragmentację i defragmentację datagramów. Za wybór trasy datagramu poprzez sieć odpowiedzialne są protokoły routingu. Routing w Internecie ma przy tym charakter hierarchiczny.

**IP jest typowym przykładem protokołu bezpołączeniowego.** Często określany jest też mianem protokołu niewiarygodnego, gdyż nie wykrywa traconych datagramów.

#### Warstwa międzysieciowa - protokół IP

Jak już wspomniano wyżej IP (ang. *Internet Protocol*), jest przykładem protokołu bezpołączeniowego. Oznacza to, iż protokół ten pozwala wymieniać informacje między dwiema stacjami roboczymi bez konieczności wcześniejszego nawiązywania sesji i ustalania jej parametrów. Mimo niewątpliwych zalet, takich jak prostota implementacji i oszczędne wykorzystanie medium transmisyjnego, rozwiązań to posiada jedną poważną wadę - IP nie zapewnia niezawodnego dostarczenia pakietów danych do odbiorcy. Wydawałoby się na pozór, iż nie jest to uciążliwe, ponieważ współczesne sieci zapewniają dużą niezawodność transmisji i niską stopę błędów. Jednak i w tych sieciach, w okresach dużego natężenia ruchu może dochodzić do przepełnienia buforów routerów, co z kolei

#### 1.3.4 Architektura TCP/IP

spowodować może odrzucanie, a tym samym utratę pakietów z danymi. Pociąga to za sobą konieczność implementacji odpowiednich metod zabezpieczających transmisję w wyższych warstwach, np. w TCP.

Warstwa międzysieciowa Internetu ukrywa przed aplikacjami istnienie fizycznej sieci i tworzy wirtualny system transportowy dla użytkownika. Z tego punktu widzenia protokół IP jest niezwykle atrakcyjny ponieważ pozwala na współpracę, poprzez sieć, szerokiego wachlarza aplikacji z wykorzystaniem jednego, standar-dowego interfejsu sieciowego. Protokół IP jest łatwy w implementacji, a poprzez swą bezpołączeniową architekturę - nieskomplikowany.

W protokole IP nie przewiduje się mechanizmów odtwarzania połączenia po awarii sieci, brak jest także kontroli przepływu pakietów. Pakiety z danymi użytkownika mogą zostać powielone lub odebrane w innej kolejności niż były wysłane, bądź - w skrajnym przypadku - zagiąć. IP realizuje za to mechanizm segmentacji pakietów. Segmentacja oznacza w tym przypadku podział pakietu danych na kilka mniejszych. Usługa tego typu jest niezwykle użyteczna w przypadku współpracy różnych sieci komputerowych. Na przykład w sieciach rozległych X.25 stosowana jest zwykle długość pakietu wynosząca 128 bajtów. Z kolei w sieciach typu Ethernet używane są zazwyczaj pakiety o długości do 1500 bajtów. Brak segmentacji zmuszałby użytkowników sieci do dopasowywania długości pakietów danych do wymagań obowiązujących w poszczególnych sieciach. Dzięki segmentacji istnieje możliwość dzielenia pakietów tak, aby mogły być one zaakceptowane przez każdą z sieci składowych Internetu. Operacja fragmentacji wymaga oczywiście zaimplementowania w stacji końcowej mechanizmu składania datagramu, gwarantującego jego poprawne zrekonstruowanie u odbiorcy.

Tabela 1.2. Znaczenie i długości pól pakietu IP

Lp.	Długość (w bajtach)	Nazwa
1	4 bity	numer wersji protokołu
2	4 bity	długość nagłówka
3	1	typ obsługi
4	2	długość całkowita
5	2	identyfikator
6	3 bity	flagi
7	13 bitów	przesunięcie
8	1	czas życia
9	1	protokół
10	2	suma kontrolna
11	4	źródłowy adres IP
12	4	docelowy adres IP
13	zmienna	opcje
14	zmienna	dane użytkownika

Nieco dokładniejszą analizę protokołu IP poprzedzimy opisem zawartości poszczególnych pól datagramu tego protokołu. Tabela 1.2 określa położenie, nazwy i długości poszczególnych pól. Poszczególne pola to:

*numer wersji* - pole to identyfikuje numer wersji protokołu IP używanego przez nadawcę. Większość protokołów IP używa tego pola ponieważ nie wszystkie stacje muszą mieć zaimplementowaną najnowszą wersję. Aktualnie używana jest wersja 4 protokołu IP (IPv4). Trwają jednak zaawansowane prace nad kolejną, 6-stą jego wersją, tj. protokołem IPv6.

*długość nagłówka* - pole to zawiera 4 bity określające wielkość nagłówka IP wyrażoną liczbą słów 32 bitowych w pakiecie danych. Wartość ta jest wykorzystywana do określenia początku nagłówka protokołu warstwy wyższej. Ponieważ typowy nagłówek IP (bez uwzględnienia opcji) ma długość 20 bajtów, w opisywanym polu znajdziemy zazwyczaj liczbę 5.

Tabela 1.3. Elementy pola Typ Obsługi

Pozycja bitów	Nazwa pola	Znaczenie
0-2	Priorytet pakietu	000 zwykły 001- priorytetowy 010 pilny 011 natychmiastowy 100 natychmiastowy przyśpieszony 101 CEITIC/ECP 110 zarządzanie globalne 111 zarządzanie lokalne
3	opóźnienie	0 zwykłe 1 małe
4	przepustowość	0 zwykła 1 duża
5	niezawodność	0 zwykła 1 wysoka
6-7	niezdefiniowane	niezdefiniowane

*typ obsługi* - pole to definiuje typy usług oferowanych przez protokół IP; wartości pola wskazują na: priorytet pakietu, opóźnienie transmisji, pożadaną przepustowość i niezawodność. W literaturze angielskiej nazwa tego pola pojawia się zwykle jako skrót TOS (ang. *type of service*). W tabeli 1.3 opisane są poszczególne wartości bitów pola TOS. TOS zawiera pięć pól, które tworzą słowo osmioróżkowe. Bity 0,1 i 2 opisują priorytet pakietu, czyli podając ważność zawartej w nim informacji. Priorytet 0 oznacza zwykły pakiet danych, priorytet 7 określa zaś pakiet o największym znaczeniu. Pole TOS jest rzadko używane, ale część implementacji „zaznacza” pakiety danych zawierające informacje kontrolne i sterujące priorytetem o wartości 7. Pole typu

obsługi TOS mogłyby być wykorzystane do kontroli ruchu i przeciążeń w sieci. Routery powinny wówczas przepuszczać pakiety o wyższym priorytecie szybciej, a w przypadku przeciążeń sieci pakiety o niskim priorytecie powinny być z niej usuwane. Niestety dopiero teraz pojawiają się pierwsze implementacje oprogramowania routerów uwzględniające TOS w procesie routingu.

Pozostałe trzy bity pola typu obsługi określają kolejno:

*bit opóźnienia* (ang. *delay bit - D*) - ustawiony bit 3 nakazuje przesyłanie pakietu IP trasą o najmniejszym opóźnieniu. Możemy sobie wyobrazić sytuację kiedy istnieją dwa łącza, jedno satelitarne o dużej przepustowości oraz drugie łącze naziemne, o znacznie mniejszej przepustowości. Normalne pakiety byłyby przesyłane przez satelitę. Te z ustawionym bitem 3 w polu TOS będą kierowane łączem naziemnym. Norma IP nie opisuje jednak opóźnienia jako takiego i pozostawia interpretację obsługi tego bitu dostawcom routerów.

*bit przepustowości* (ang. *throughput bit - T*) - ustawiony bit 4 poleca przesyłać datagram po łączach o możliwie największej przepustowości. Podobnie jak w poprzednim przypadku, norma nie definiuje pojęcia łącz o największej przepustowości i interpretacja sposobu obsługi tego bitu pozostaje w gestii producentów routerów,

*bit niezawodności* (ang. *reliability bit - R*) - ustawiony bit 5 zaleca przesyłać pakiet łączem o największej niezawodności. Znaczenie słowa „niezawodność” także nie jest definiowane,

*bit 6 i 7* - nie zostały jeszcze zdefiniowane i są zarezerwowane do przyszłego wykorzystania,

*długość całkowita* - pole to określa całkowitą długość pakietu IP wraz z nagłówkiem w bajtach. Maksymalna długość pakietu IP wynosi przy tym 65535 bajtów. Routery obsługujące pakiety IP muszą być przygotowane do obsługi pakietów o największej dopuszczalnej długości dla danej sieci fizycznej, do której są podłączone. Niezależnie od tego każdy router IP powinien obsługiwać pakiety o długości co najmniej 576 bajtów.

Pola: *identyfikatora, flagi i przesunięcia w pakiecie* służą do kontroli segmentacji pakietów. Pole identyfikatora zawiera unikatowy identyfikator, wspólny dla wszystkich fragmentów jednego pakietu. W zestawieniu z adresem źródłowym w nagłówku pole to umożliwia odbiorcy jednoznaczna identyfikację wszystkich fragmentów jednego pakietu, a tym samym poprawną jego rekonstrukcję. Pole *flagi* steruje procesem fragmentacji:

- bit 0 - niezdefiniowany,
- ustawiony bit 1 zabrania fragmentacji pakietu,
- ustawiony bit 2 oznacza, iż nie jest to ostatni fragment pakietu i należy spodziewać się następnych.

Pole *przesunięcia w pakiecie* podaje jak daleko, licząc od początku pakietu, należy umieścić ten fragment. Pierwszy fragment ma przesunięcie 0, które jest zwiększane o długość fragmentu w miarę wysyłania kolejnych „porcji”.

*czas życia* (ang. TTL - *Time To Live*) - pole to pomaga routery mierzyć czas, przez jaki pakiet pozostaje w sieci. Obecna implementacja IP nakazuje każdemu z routerów, na drodze pakietu, zmniejszanie wartości zawartej w polu TTL o jeden, a w przypadku gdyby pole TTL osiągnęło wartość 0 - usunięcie pakietu z sieci. Niewykluczone, iż w przyszłości pole TTL będzie zmniejszane w jednosekundowych odstępach, co w pełni uzasadni jego nazwę. Podstawowym zastosowaniem opisywanego pola jest likwidacja „zapętlonych” ramek. Niekiedy błędy w tablicach routerów powodują powstawanie pętli w sieci. Pomimo, iż sytuacje takie zdarzają się bardzo rzadko, brak jakiegokolwiek mechanizmu wykrywania kräążących ramek doprowadziłby do tego, że z czasem sieć wypełniłaby się bezużytecznym ruchem. Dzięki TTL istnieje pewność, iż po przejściu maksymalnie 255 routerów pakiet zostanie usunięty z sieci.

*protokół* - pole to definiuje następny w hierarchii protokół zawarty w pakiecie danych. Typy poszczególnych protokołów są zakodowane według norm IP i przedstawione w tabeli 1.4.

Tabela 1.4. Identyfikatory typu protokołu IP

Numer protokołu	Skrót nazwy	Nazwa
0		zarezerwowane
1	ICMP	Internet Control Message Protocol
2	IGMP	Internet Group Management Protocol
3	GGP	Gateway to Gateway Protocol
4		bez przydziału
5	ST	Stream
6	TCP	Transmission Control Protocol
7	UCL	UCL
8	EGP	Exterior Gateway Protocol
9	IGP	Interior Gateway Protocol
10	BBN-MON	BBN-RCC Monitor
11	NVP	Network Voice Protocol
12	PUP	PUP
13	ARGUS	ARGUS
14	EMCON	EMCON
15	XNET	Cross Net Debugger
16	CHAOS	Chaos
17	UDP	User Datagram Protocol
18	MUX	Multiplexing
19	DCN-MEAS	Multiplexing

Tabela 1.4. Identyfikatory typu protokołu IP (c.d.)

Numer protokołu	Skrót nazwy	Nazwa
20	HMP	Host Monitoring Protocol
21	PRM	Packet Radio Monitoring
22	XNS-IDP	Xerox NS IDP
23	TRUNK-1	Trunk-1
24	TRUNK-2	Trunk-2
25	LEAF-1	Leaf-1
26	LEAF-2	Leaf-2
27	RDP	Reliable Data Protocol
28	IR TP	Internet Reliable TP
29	ISO-TP4	ISO Transport Class 4
30	NETBLT	Bulk Data Transfer
31	MFE-NSP	MFE Network Services
32	MERIT-INP	Merit Internodal Protocol
33	SEP	Sequential Exchange Protocol
34-60		bez przydziału
61		Internal protocols
62	CFTP	CFTP
63		Local Network Protocol
64	SAT	SatNetProtocol
65	MIT-SUBN	MIT Subnet Report
70		bez przydziału
71	IPCV	Packet Core Utility
72-75		bez przydziału
76	BRSAT-MON	Backroom Satnet Monitoring
77		bez przydziału
78	WB-MON	Wideband Monitoring
79	WB EXPACK	Wideband Expack
80-254		bez przydziału

*suma kontrolna* - pole to używane jest do kontroli poprawności informacji zawartej w nagłówku ramki danych protokołu IP. Sumą kontrolną nie jest objęta część pakietu zawierająca dane użytkownika. Sposób obliczania sumy kontrolnej jest zdefiniowany w odpowiednim dokumencie RFC. Suma jest obliczana przez nadawcę pakietu i powinna być kontrolowana przez poszczególne routery transmitujące pakiet oraz przez odbiorcę. Niestety niektóre

pakiety programowe obsługujące protokoł IP nie sprawdzają sumy kontrolnej, co może prowadzić do nieoczekiwanej zachowania się stacji roboczej, która odebrała zniekształcony pakiet.

Dwa kolejne pola zawierają adresy IP nadawcy i odbiorcy pakietu. Format adresów i ich interpretacja zostaną opisane w kolejnym podpunkcie.

Zawartość pola *opcje* opisana jest w tabeli 1.5.

Tabela 1.5. Elementy pola Opcje

Klasa	Numer	Długość	Opis
0	0	0	koniec listy
0	1	0	element pusty
0	2	11	bezpieczeństwo
0	3	zmienna	loose source routing
0	7	zmienna	zapamiętaj drogę
0	8	4	identyfikator strumienia
0	9	zmienna	dokładny source routing
2	4	zmienna	znacznik czasowy

Innym z protokołów zdefiniowanych w warstwie międzysieciowej jest ICMP.

#### Protokół ICMP sterowania pracą sieci Internet

Jak podkreślane już poprzednio, *protokół IP nie posiada żadnych mechanizmów umożliwiających kontrolę pracy sieci. W celu realizacji tych mechanizmów stworzony został protokół ICMP (ang. Internet Control Management Protocol) pozwalający na wymianę informacji o stanie sieci.*

Protokół ICMP wspomaga:

- sterowanie przepływem (odbiorca może wysłać do nadawcy żądanie chwilowego wstrzymania nadawania),
- wykrywanie nieosiągalnych miejsc przeznaczenia (pośredni router lub docelowy komputer mogą wysłać do źródła datagramów komunikat o niemożności odbierania danych przez - odpowiednio - sieć/komputer lub port),
- routowanie (router może wysłać informację, że lepszym pośrednikiem w transmisji danych jest inny router przyłączony do tej samej sieci),
- sprawdzanie sprawności oddalonego systemu.

Nagłówek protokołu ICMP zawiera typ wiadomości, pole z informacją o zgłoszonym kodzie błędu oraz sumę kontrolną zabezpieczającą całą wiadomość ICMP (patrz tabele 1.6, 1.7 i 1.8). Komunikaty pakietów są przesyłane wewnątrz datagramów IP.

Tabela 1.6. Znaczenie i zawartość pól pakietu ICMP

Lp.	Długość (w bajtach)	Nazwa
1	1	typ wiadomości
2	1	kod błędu
3	2	suma kontrolna
4	zmienna	parametry
5	zmienna	dane użytkownika

Opis pól:

- Typ wiadomości - szczegółowy opis zawarto w tabeli 1.7.
- Kod błędu - szczegółowy opis zawarto w tabeli 1.8.
- Suma kontrolna - suma z uzupełnieniem do jedynki wszystkich pól nagłówka i pola danych.
- Parametry, jeżeli występują.
- Dane użytkownika.

Tabela 1.7. Opis pola Typ wiadomości

Numer typu	Typ wiadomości
0	Odpowiedź na Echo
3	Adresat nieosiągalny
4	Łącze zajęte
5	Przelączenia
8	Żądanie Echo
11	Czas przekroczony
12	Zły parametr
13	Żądanie znacznika czasowego
14	Odpowiedź na żądanie znacznika czasowego
15	Żądanie informacyjne
16	Odpowiedź na żądanie informacyjne
17	Żądanie maski
18	Odpowiedź na żądanie maski

Tabela 1.8. Opis pola Kod błędu

Kod błędu	Opis
0	Sieć niedostępna
1	Stacja niedostępna
2	Protokół nie jest obsługiwany
3	Port zajęty
4	Konieczna fragmentacja
5	Zła specyfikacja ścieżki

W przypadku testowania kanału łączności między dwiema stacjami Internetu używane są wiadomości typu żądanie odpowiedzi (ang. *request Echo*) i odpowiedź na to żądanie. Żądanie, *request Echo*, zawiera numer sekwencyjny oraz pewną liczbę danych. Po odebraniu żądania adresat odsyła odpowiedź Echo z tym samym numerem sekwencyjnym i tymi samymi danymi, które otrzymał w żądaniu. Dzięki temu stacja wysyłająca żądanie może, porównując otrzymane dane ze swoim wzorcem, określić czy zostały one przesłane przez sieć bezbłędnie.

#### **Adresacja w IP**

W celu przesyłania danych między dwiema aplikacjami, współpracującymi między sobą poprzez sieć Internet, protokoły TCP/IP stosują specjalne mechanizmy adresacji. Mechanizmy te zapewniają identyfikację komputera w sieci (adres IP), określając właściwy proces aplikacyjny w komputerze poprzez numerację protokołów i portów. Powyższy sposób adresowania efektywnie wspomaga procesy doboru tras.

**W chwili obecnej (zgodnie z wersją 4 protokołu IP) do adresowania komputerów i sieci IP używa 32 bitowego adresu - identyfikującego jednoznacznie każde z urządzeń, pracujących w sieci.** Adres ten składa się z dwóch elementów - numeru sieci oraz numeru komputera w sieci, przy czym wielkość tych elementów mogą się zmieniać. Decyduje o tym tzw. maska, która jest także 32 bitowym ciągiem, posiadającym wartość jeden na pozycjach bitów odpowiadających numerowi sieci, a wartość zero na pozycjach bitów określających numer urządzenia w sieci. Maska nie jest przesyłana wraz z pakietem IP. Konieczne jest więc jej odtwarzanie na podstawie parametrów konfigurowanych w routerach i stacji odbiorcy.

Warto nadmienić, że adres IP wyznacza nie tylko samo urządzenie ale identyfikuje sieć, do której owo urządzenie jest podłączone. Konsekwentnie zatem, przeniesienie urządzenia do innej sieci pociąga za sobą zmianę numeru IP. Przeniesienie takie może też wymagać zmiany maski lub typu adresu IP.

Adresy IP dzieli się na cztery klasy, nazywane odpowiednio klasami A, B, C i D (patrz rysunek 1.14). Podział ten, określany też mianem podziału kanonicznego, pozwala na ustalenie długości elementu zawierającego numer sieci i elementu zawierającego numer komputera w sieci, bez potrzeby znajomości maski.

Klasa A	0	numer sieci (7 bitów)	numer urządzenia (24 bity)
Klasa B	10	numer sieci (14 bitów)	numer urządzenia (16 bitów)
Klasa C	110	numer sieci (21 bitów)	numer urządzenia (8 bitów)
Klasa D	1110	adres rozgłoszeniowy (28 bitów)	

Rys. 1.14. Postacie kanoniczne adresów IP

Adresy klasy A nadawane są sieciom o dużej liczbie komputerów. W tym przypadku, część adresu określająca numer urządzenia ma długość 24 bitów. Pozwala to na zaadresowanie do  $2^{24}$  urządzeń lub komputerów. Tak duża liczba możliwych adresów w sieci pociąga za sobą konieczność ograniczenia liczby samych sieci. W klasie A można zaadresować jedynie 127 sieci. Widać więc, iż adresy tej klasy można wykorzystać w systemie z małą liczbą sieci dużych rozmiarów (czyli o dużej liczbie stacji końcowych).

Dla mniejszych sieci, o średnim rozmiarze, stosuje się adresy klasy B. Długość części sieciowej wynosi wtedy 14 bitów. Pozwala to na adresację 16382 sieci. Długość pola zawierającego numer urządzenia wynosi w adresach klasy B 16 pozycji. Umożliwia to zaadresowanie w każdej z tych sieci do 65534 komputerów. W przypadku adresów klasy C długość części „sieciowej” zwiększana jest do 21 bitów. Tylko 8 bitów przypada wtedy na numer urządzenia.

W tabeli 1.9 podano ilości sieci i urządzeń jakie mogą zostać zaadresowane w ramach poszczególnych klas adresów IP.

Tabela 1.9. Ilość sieci i urządzeń dla poszczególnych klas adresów IP

	ilość sieci	ilość urządzeń
Klasa A	126	16 777 124
Klasa B	16 384	65 534
Klasa C	2 097 152	254

Kolejna klasa adresów, czyli klasa D, nie jest przeznaczona do adresowania urządzeń. Używa się jej do tworzenia adresów rozgłoszeniowych dla grup odbiorców.

Dla celów organizacji pracy sieci zarezerwowano grupę adresów, które są niedostępne dla użytkowników. Są to np. adresy sieci, których pierwszy bajt jest większy od 223 lub którego wartość jest równa 0 (adres 0 oznacza tzw. trasę domyślną, 127 - adres własny sieci). W systemie adresacji IP wydzielono również specjalną grupę adresów komputerów, które mają ściśle określone znaczenie np. 0 - oznacza „samego siebie” w sieci, a 255 jest adresem rozgłoszeniowym.

Jak wspomniano, celem realizacji Internetu było zapewnienie właściwych asocjacji wielu procesów aplikacyjnych z kilkoma protokołami transportowymi, jak też integrację tych protokołów transportowych z protokołem Internet. W tym celu, w TCP/IP wprowadzono numerację protokołów (jeden bajt umieszczony w trzecim słowie nagłówka IP - patrz tabele 1.2 i 1.4) i numery portów (dwa bajty umieszczone w pierwszym słowie nagłówka segmentu). Zarezerwowało przy tym grupę protokołów i numery portów dla tzw. dobrze znanych usług (np. TELNET - 23/tcp; FTP - 21/tcp; WHO - 513/udp).

Kombinacja 4-bajtowego adresu IP i numeru portu nosi nazwę gniazdka (ang. *socket*). Para gniazdek przyporządkowanych współpracującym procesom aplikacyjnym w komputerach: źródłowym i docelowym jednoznacznie definiuje połączenie TCP.

Należy tutaj zwrócić uwagę na fakt, że **opracowana ostatnio przez IETF nowa wersja protokołu IP, IPv6, definiuje adresy 128 bitowe**. Opis nowego schematu adresacji znajduje się w rozdziale 8 książki.

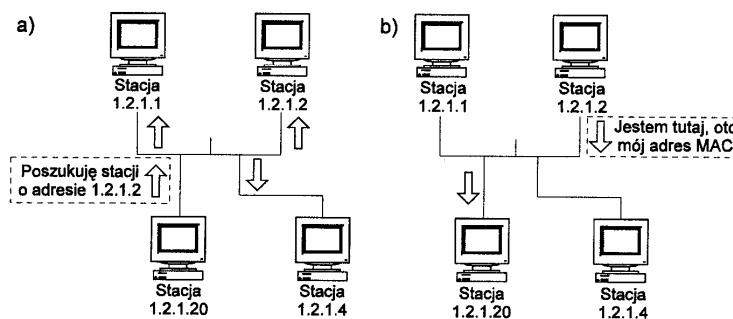
#### Protokół ARP konwersji adresów IP na adresy fizyczne

Chcąc dostarczyć wiadomość do adresata o znanym adresie IP stajemy przed koniecznością wyznaczenia jego adresu MAC-owego. Dysponując jedynie adresem IP nie mamy możliwości określenia tego adresu, zwłaszcza, że adresy IP mogą się zmieniać, w zależności od lokalizacji stacji w sieci. Aby rozwiązać ten problem, opracowany został specjalny protokół, zwany w skrócie ARP (ang. *Address Resolution Protocol*). Dzięki niemu szczegóły implementacyjne dotyczące rodzaju medium i fizycznej adresacji są ukryte i niezależne od oprogramowania wyższych warstw.

Generalnie ARP pracuje w oparciu o specjalną, wewnętrzną tablicę zawierającą pary adresów IP i adresów MAC jednoznacznie ze sobą powiązanych. Kiedy sterownik karty sieciowej zwraca się do programu obsługi protokołu ARP, ten przegląda tablice i sprawdza, czy dany adres IP jest odnotowany w tej tablicy. W przypadku znalezienia adresu IP protokół ARP przesyła zwróciście odpowiadający mu adres MAC. W przeciwnym przypadku zachodzi konieczność wysłania do sieci specjalnego pakietu rozgłoszeniowego, zwanego żądaniem/wywołaniem protokołu ARP.

Ponieważ wywołanie ARP jest rozsyłane przez router na adres rozgłoszeniowy, odbierają je wszystkie stacje położone w lokalnej sieci IP. Każda ze stacji porównuje wtedy adres IP zawarty w wywołaniu ARP ze swoim adresem IP i w przypadku zgody odsyła do stacji wywołującej odpowiedź ARP. Odpowiedź ARP różni się od wywołania tylko jednym istotnym szczegółem - zawiera adres MAC stacji wywoływanej, który jest następnie wstawiany do wewnętrznej tablicy stacji wywołującej.

Dzięki temu, iż wywołanie ARP zawiera adres IP i adres MAC stacji wywołującej, stacja wywoływana może także uaktualnić swoją tablicę wewnętrzną, przygotowując się do nawiązania komunikacji.



Rys. 1.15. Ilustracja działania protokołu ARP

#### 1.3.4 Architektura TCP/IP

Rysunek 1.15 obrazuje proces poszukiwania adresu MAC stacji wywoywanej. Stacja o adresie IP 1.2.1.20 poszukuje adresu MAC stacji o adresie IP 1.2.1.2. Generuje więc ona wywołanie ARP. Wszystkie stacje w segmencie odbierają to wywołanie, ale tylko ta o adresie 1.2.1.2 ma prawo na nie odpowiedzieć (patrz rysunek 1.15a). Na rysunku 1.15b widzimy jak stacja 1.2.1.2 odpowiada na wywołanie, przesyłając swój adres MAC. Odpowiedź na wywołanie kierowana jest bez rozgłaszenia, bezpośrednio na adres MAC stacji wywołującej.

Format pakietu ARP stosowany przy poszukiwaniu stacji o adresie MAC przedstawiono w tabeli 1.10.

Tabela 1.10. Format pakietu ARP

Lp.	Długość (w bajtach)	Nazwa
1		Nagłówek medium transmisyjnego, np. Ethernet
2	2	Typ medium transmisyjnego
3	2	Typ protokołu
4	1	Długość adresu sprzętowego (n)
5	1	Długość adresu protokołowego (m)
6	2	Typ operacji
7	n	Adres sprzętowy stacji wywołującej
8	m	Adres protokołowy stacji wywołującej
9	n	Adres sprzętowy stacji wywoywanej
10	m	Adres protokołowy stacji wywoywanej

Opis poszczególnych pól pakietu ARP.

1. Nagłówek medium transmisyjnego - zależy od typu stosowanego medium np. Token Ring
2. Typ medium transmisyjnego - szczegółowy opis zawarto w tabeli 1.10
3. Typ protokołu - zazwyczaj 0806 hex
4. Długość adresu sprzętowego - wyrażona w bajtach
5. Długość adresu protokołowego - wyrażona w bajtach
6. Typ operacji - wartość 1 dla wywołania ARP i 2 dla odpowiedzi na wywołanie 7,8,9,10 Adresy - odpowiednie adresy według długości ustalonych w polach 4 i 5

Tabela 1.11. Zawartość pola Typ medium pakietu ARP

Numer	Typ medium
1	Ethernet 10 Mb
2	Ethernet eksperymentalny 3 Mb
3	radiowy X.25
4	Proteon ProNET Token Ring
5	Chaos
6	sieci IEEE 802
7	ARCNET

Podanie w pakiecie ARP typu medium transmisyjnego pozwala odbiorcy na ustawienie parametrów sesji, np. maksymalnego czasu przesyłania danych itp. Możliwe typy medium wyszczególniono w tabeli 1.11.

### Warstwa transportowa

Protokół IP jest protokołem sieciowym, oznacza to, iż nie jest on bezpośrednio udostępniany aplikacjom do przesyłania danych. Dopiero wyższa warstwa protokołarna obejmująca protokoły TCP i UDP zapewnia interfejs bezpośrednio widoczny dla innych elementów systemu komputerowego.

**Protokół TCP (ang. Transmission Control Protocol) realizuje transmisję w trybie połączeniowym.** Zapewnia kontrolę poprawności pakietów, w tym retransmisję pakietów zaginionych, usuwanie pakietów zduplikowanych oraz porządkowanie kolejności pakietów odbieranych. Korzystając z protokołu TCP budowane są bardziej zaawansowane protokoły aplikacyjne - protokół transmisji plików FTP, emulacja terminala sieciowego TELNET, protokół wymiany poczty SMTP (ang. Simple Mail Transmission Protocol) oraz protokół komunikacyjny systemu okienkowego Xwindows.

**Protokół TCP dostarcza, zorientowany połączeniowo, niezawodny system transmisji.** Fakt ten jest okupiony zarówno dość skomplikowanym i rozbudowanym sposobem obsługi, jak i odpowiednio dużym nagłówkiem pakietu, zawierającym wszystkie informacje, niezbędne do synchronizacji sesji i wykrywania ewentualnych błędów.

Okazuje się, że w sieciach często występują sytuacje, w których stosowanie rozbudowanego protokołu TCP jest niecelowe, np.:

1. przy przesyłaniu bardzo małych ilości danych efektywniejsza może być retransmisja całego bloku danych niż realizacja procedur TCP zestawiania połączenia i zapewniania niezawodnego przekazu,
2. wysyłając poprzez sieć krótkie zapytania i oczekując krótkich odpowiedzi w sposób naturalny można traktować uzyskanie odpowiedzi jako powiadomienie pozytywne, a brak tej odpowiedzi jako brak potwierdzenia i żądanie retransmisji zapytania,
3. niektóre aplikacje we własnym zakresie zapewniają niezawodne dostarczanie danych.

Na potrzeby pewnych aplikacji stworzono więc protokół UDP (ang. User Datagram Protocol) o bardzo skromnych możliwościach protekcyjnych, ale za to o małym stopniu złożoności.

**UDP dostarcza prostego, zorientowanego bezpołączeniowo systemu transmisji pakietów.** Ponad protokołem UDP zaimplementowano najprostsze odmiany protokołów aplikacyjnych - protokół zarządzania SNMP (ang. Simple Network Management Protocol), protokół służący do przesyłania plików TFTP (ang. Trivial File Transmission Protocol) oraz realizację zdalnych wywołań procedur RPC

(ang. Remote Procedure Call) wraz z opartym na niej sieciowym systemem plikowym NFS (ang. Network File System).

Tabela 1.12. Znaczenie i długości pól pakietu UDP

Lp.	Długość (w bajtach)	Nazwa
1	2	numer portu źródłowego
2	2	numer portu docelowego
3	2	długość
4	2	suma kontrolna
5	zmienna	dane użytkownika

UDP nie zapewnia niezawodnego dostarczenia pakietu do odbiorcy ani nie pozwala na wykrycie powielenia pakietu lub zmiany kolejności pakietów po stronie odbiorcy; jedynie suma kontrolna w nagłówku UDP eliminuje pakiety uszkodzone w czasie transmisji. Strukturę pakietu protokołu UDP przedstawiono w tabeli 1.12. Znaczenie poszczególnych pól pakietu jest następujące:

1. Numer portu źródłowego - identyfikuje aplikację wysyłającą pakiet. Jest to pole opcjonalne, jeżeli nie jest używane, to domyślnie wstawiana jest wartość zero.
2. Numer portu docelowego - identyfikuje aplikację lub proces docelowy w systemie odbiorcy.
3. Długość - całkowita długość pakietu UDP - suma długości nagłówka UDP i pola danych.
4. Suma kontrolna - suma z uzupełnieniem do jedynki wszystkich pól nagłówka i pola danych. Jeżeli ramka wymaga tzw. wypełnienia, ponieważ np. jest zbyt krótka do wysłania przez dane medium (Ethernet wymaga by ramka miała co najmniej 64 bajty) to suma kontrolna jest obliczana wraz z wypełnieniem.
5. Dane użytkownika.

Należy przy tym zwrócić uwagę na to, że oba protokoły transportowe tj. TCP i UDP są stosunkowo mało wydajne. Zostały one bowiem zaprojektowane do wykorzystania w środowisku sieciowym na przełomie lat 70-tych i 80-tych i dostosowane do potrzeb ówczesnych „mało wymagających” aplikacji oraz wysoce zawodnych podsieci komunikacyjnych. Protokoły te są obecnie usprawniane poprzez wprowadzanie prostszych, a przez to efektywniejszych mechanizmów sterowania przepływem danych, tak by mogły one sprostać nowym wymaganiom stawianym przez szybkie aplikacje multimedialne, w tym zagwarantować możliwość negocjacji parametrów charakteryzujących jakość transmisji, czy też realizacji połączeń wielopunktowych. Prowadzone są też prace badawcze i próby implementacji szybkich a jednocześnie elastycznych protokołów transportowych. Protokoł typu XTP (ang. eXpress Transfer Protocol) mający zastąpić TCP oraz

UDP, a także wiele innych specjalizowanych protokołów transportowych (np. protokół SPP (ang. *Sequenced Packet Protocol*) z rodziny XNS (ang. *Xerox Network System*) dopuszczają uproszczone procedury zestawiania i rozłączania połączeń oraz definiują możliwość przesyłania standardowych bloków danych i ich równoległego przetwarzania na kilku procesorach. W wyniku tych (i szeregu innych) modyfikacji możliwa staje się obsługa pakietów, przez protokoły transportowe, w czasie porównywalnym z czasami transmisji pakietów w medium.

Nie ulega wątpliwości, że właściwie zaprojektowany protokół transportowy ma zasadniczy wpływ na możliwość implementacji a także na wydajność realizacji aplikacji.

#### **Warstwa aplikacji w modelu TCP/IP**

Najwyżej położoną warstwą w hierarchii TCP/IP jest warstwa aplikacji (ang. *application layer*), w której rezydują procesy i protokoły użytkowe. Wszystkie one używają do przesłania swoich danych protokołów warstwy transportowej. Procesy użytkowe identyfikowane są przez 16-bitowy numer portu. Każdy z segmentów TCP lub pakietów UDP zawiera numer portu źródła oraz numer portu docelowego. Pierwszy z tych numerów identyfikuje proces wysyłający dane, drugi - proces do którego są one kierowane. Numery portów mogą nie być unikatowe, nie mogą się jedynie powtarzać numery związane z tym samym protokołem transportowym. Oznacza to, że protokoły TCP i UDP korzystają z tych samych numerów portów do obsługi różnych procesów; jednak numery portów przypisane tylko do protokołu TCP muszą być przy tym różne. Wynika stąd, że jedynie para protokół transportowy i numer portu nazwana gniazdkiem (ang. *socket*) jednoznacznie identyfikuje proces docelowy. Najbardziej znanymi protokołami użytkowymi są: protokół przekazu plików FTP (ang. *File Transfer Protocol*) używany do przesyłania plików, protokół wirtualnego terminala TELNET (ang. *Network Terminal Protocol*), umożliwiający rozpoczęcie sesji za pośrednictwem sieci, protokół SMTP dostarczający pocztę elektroniczną (ang. *Simple Mail Transfer Protocol*). W warstwie tej znajdują się również aplikacje takie jak serwer nazw DNS (ang. *Domain Name Service*), sieciowy system plików NFS (ang. *Network File System*), czy protokół informacji routingowych RIP (ang. *Routing Information Protocol*), o istnieniu których normalny użytkownik może nie mieć pojęcia, a stanowiących kluczowe elementy gwarantujące prawidłowe działanie całej sieci. Serwer nazw dokonuje zamiany nazw urządzeń działających w sieci na odpowiadające im adresy sieciowe. Sieciowy system plików umożliwia współdzielenie plików przez wiele komputerów w sieci. Protokół RIP jest wykorzystywany do wymiany informacji routingowych używanych do określenia tras przesyłania danych. RIP korzysta z usług protokołu UDP.

Przesyłanie plików odbywa się przy użyciu protokołu FTP. Autoryzowany użytkownik, posiadający konto i dostęp do określonego obszaru pamięci serwera, może przesyłać dowolny zbiór z (do) tego obszaru do (ze) swojego komputera lokalnego. Do tego celu wykorzystuje się współdziałanie dwóch partnerów:

usługodawcy i usługobiorcy. Usługodawca odpowiedzialny jest za utworzenie połączenia (nawiązanie asocjacji), dostarcza danych niezbędnych do autoryzacji dostępu, określa tryb przesyłania i nazwę pliku. Usługobiorca uczestniczy w nawiązaniu asocjacji, sprawdza autoryzację dostępu i nadzoruje przesyłanie. Połączenie polega na jednoczesnym utworzeniu dwóch wirtualnych kanałów: pierwszego, służącego do przesyłania danych i drugiego, przeznaczonego do celów nadzorujących. Protokół FTP korzysta bezpośrednio z usług warstwy transportowej, a konkretne - protokołu TCP. Umożliwia on przesyłanie plików w obydwu kierunkach, tj. od usługobiorcy do usługodawcy (otrzymując w ten sposób prawo do zapisania pliku) i od usługodawcy do usługobiorcy (prawo do odczytania pliku).

Do realizacji usługi poczty elektronicznej opracowano protokół SMTP. Umożliwia on przesyłanie dowolnych wiadomości reprezentowanych jako ciągi znaków ASCII.

W przeciwieństwie do modelu ISO/OSI, gdzie część funkcji realizowanych jest w wydzielonych stacjach, w TCP/IP wszystkie funkcje realizowane są w stacjach końcowych. Protokół SMTP korzysta z usług transportowych protokołu TCP. Moduł transmisyjny jest odpowiedzialny za przekaz wiadomości aż do momentu jej rozesłania do wszystkich stacji przeznaczenia. Wówczas treść wiadomości w stacji źródłowej ulega skasowaniu, a za wiadomość odpowiedzialny staje się moduł transmisyjny stacji przeznaczenia. Transmisja między tymi modułami odbywa się na zasadzie „wyślij i czekaj” co powoduje, iż protokół ten nie chroni ani przed powieleniem ani też przed zagubieniem wiadomości. Nadawca wiadomości nie otrzymuje żadnego powiadomienia pozytywnego bądź negatywnego odebrania wiadomości. Jedynie niektóre opcje pozwalają kierować wysłane wiadomości również na ekran konsoli odbiorcy, pod warunkiem jednak, że był on aktywny.

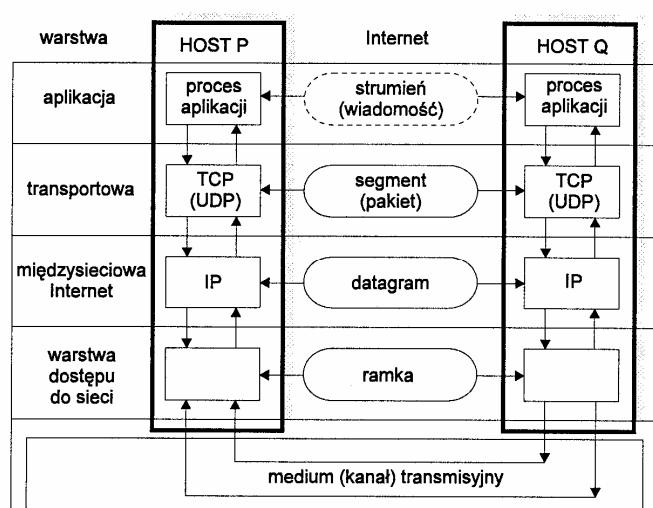
Usługa DNS umożliwia tłumaczenie nazw urządzeń sieciowych na adresy w oparciu o rozproszony system baz danych. Informacja o wszystkich stacjach nie jest zgromadzona w jednej bazie danych, ale w serwerach nazw (ang. *Name servers*) i jest udostępniona tylko tej stacji, która wyśle zapytanie. System DNS opiera się na koncepcji domen (czyli obszarów) tworzących strukturę drzewa. Na szczytce znajduje się domena korzeń obsługiwana przez serwery korzenie. Pod nią znajdują się domeny najwyższego poziomu: geograficzne (związane z obszarami państw na świecie z wyjątkiem Stanów Zjednoczonych) lub organizacyjne (określone na podstawie typu organizacji, która jest właściwicielem systemu). Zasada działania systemu DNS polega na zadawaniu pytań i uzyskiwaniu odpowiedzi. Żaden z serwerów nie ma kompletnej informacji o wszystkich domenach, wszystkie natomiast posiadają wskazówki, do kogo należy przesyłać zapytanie. Jeżeli serwer DNS otrzyma zapytanie dotyczące hosta na temat, na który nie posiada informacji, wysyła pytanie do tego serwera, który jest odpowiedzialny za posiadanie kompletnej informacji o interesującej domenie. Wyróżniamy dwa rodzaje zapytań: rekurencyjne i nierekurencyjne. W zapytaniach nierekurencyjnych

zdalny serwer udziela jedynie odpowiedzi, który serwer należy zapytać w następnej kolejności. Lokalny serwer musi więc sam wysyłać zapytania do kolejnych serwerów tak długo, aż uzyska poszukiwaną informację. W przeszukiwaniu rekurencyjnym, zdalny serwer sam przeprowadza proces przepisywania serwerów i przekazuje odpowiedzi lokalnemu serwerowi. Po uzyskaniu odpowiedzi lokalny serwer przekazuje ją zainteresowanemu i jednocześnie zachowuje tę odpowiedź w swojej bazie danych. Jeśli następnym razem otrzyma zapytanie o ten sam host, będzie już mógł sam udzielić odpowiedzi.

Usługę wirtualnego terminala realizuje protokół TELNET w oparciu o usługę transmisji połączeniowej protokołu TCP. Połączenie za pośrednictwem TELNETu umożliwia pracę na odległym komputerze poprzez sieć. System lokalny jest traktowany jedynie jako terminal w stosunku do zdalnego komputera, na którym w rzeczywistości przeprowadzane są wszelkie operacje. Usługa ta jest często wykorzystywana do połączenia dwóch odległych terminali sieciowych, znajdujących się w dowolnych węzłach sieci Internet.

Ukazujące się kolejne dokumenty RFC świadczą o ciągłym rozwoju Internetu, a więc i protokołów TCP/IP. W czterowarstwowym modelu TCP/IP 100 protokołów warstw wyższych korzysta z usług protokołu IP. Z dokumentów RFC opublikowanych w 1995 roku wynika np. że nowa wersja protokołu IP (IPv6) już wkrótce zastąpi wersję poprzednią. Opisowi tej wersji, wraz z uwagami na temat możliwości oferowanych przez IPv6, poświęcony zostanie rozdział 8 książki.

### Struktury danych



Rys. 1.16. Protokoły i jednostki danych warstw architektury TCP/IP

Każda z warstw TCP/IP posiada niezależne jednostki danych. Na rysunku 1.16 przedstawiono nazwy tych jednostek. I tak:

- Aplikacje korzystające z protokołu TCP operują na strumieniach (ang. *streams*), a aplikacje używające protokołu UDP operują na wiadomościach (ang. *messages*).
- W warstwie transportowej protokół TCP przesyła swoje dane jako segmenty, a UDP - jako pakiety.
- Z kolei w warstwie Internetu dane są traktowane jako datagramy.
- Ponieważ TCP/IP może być wykorzystywane w wielu typach sieci fizycznych, więc i terminy określające struktury danych mogą tam być bardzo różne. Zwykle jednak w warstwie łącza danych operujemy pojęciem ramki.

### 1.3.5 Perspektywy rozwoju architektur sieciowych

Wszystkie prezentowane w rozdziale 1 architektury logiczne rozległych sieci komputerowych mają swoje pełne lub częściowe (w postaci tzw. profili) implementacje. Dla przykładu architektury SNA i DEC są rozwiązaniemi o istotnym znaczeniu w USA; pod koniec lat 80-tych można było nawet mówić o dominującej roli pierwszej z nich na rynku amerykańskim. Jeszcze kilka lat temu wydawało się, że główną rolę, wśród czterech przedstawionych w tym rozdziale architektur pełnić będzie propozycja ISO-OSI. Ścisła współpraca ISO i środowiska reprezentującego DECnet zaowocowała bowiem implementacją, w sieciach firmy DEC, dwustosowej architektury tj. zestawów protokołów i aplikacji ISO-OSI i firmowego DNA. Prowadzone też były wstępne rozmowy pomiędzy ISO a reprezentantami Internetu na temat wzajemnej współpracy.

*Nieoczekiwany sukces komercyjny Internetu sprawił jednak, iż przewidywania o stałej ewolucji innych architektur w kierunku siedmiowarstwowej architektury modelu OSI wydają się w chwili obecnej mało realne, a obserwowana stała tendencja wzrostu znaczenia zestawu TCP/IP świadczyć może o pewnej degradacji znaczenia modelu ISO-OSI.*

Pojawiająca się w literaturze fachowej i wyrażana przez użytkowników sieci krytyka i surowa ocena modelu ISO-OSI wynika między innymi ze złożoności tego modelu i dużej nadmiarowości elementów organizacyjno-sterujących, wprowadzanych przez poszczególne warstwy tej architektury. W wyniku procesu przetwarzania poszczególnych jednostek danych w kolejnych warstwach nagłówki tych jednostek ulegają znacznemu rozbudowaniu, mogąc stanowić łącznie nawet 80% zawartości ramek przesyłanych do warstwy fizycznej. Innym, podkreślanym często, mankamentem OSI jest złożony sposób realizacji procesów przetwarzania danych, a fakt, że w większości implementacji sieci OSI (sieci X25, Frame Relay czy np. ISDN) przekaz danych odbywa się w trybie połączeniowym, wpływa na istotne wydłużenie czasu tego przekazu.

Należy jednakże silnie zaakcentować fakt, iż rola modelu OSI nie przestaje być ważna, z racji stosowania wielu protokołów ISO-OSI w publicznych sieciach pakietowych jak też szeregu profilach, choćby MAP bądź TOP, implementowanych w sieciach LAN w środowiskach przemysłowych i biurowych. Byłoby więc dużą przesadą twierdzenie, że znaczenie ISO-OSI jest jedynie dydaktyczne - w zakresie mechanizmów współpracy warstwowej i międzywarstwowej, definicji usług, specyfikacji protokołów, itp. Tym bardziej, że dominujący ostatnio model TCP/IP nie jest również wolny od wad. Brak w modelu TCP/IP precyzyjnie zdefiniowanych zasad współpracy warstwowej i międzywarstwowej, sprawia poważne problemy przy formalnej specyfikacji i implementacji protokołów. Istotną komplikację stanowi też brak mechanizmów gwarantujących niezawodność przekazu ramek w warstwie dostępu do sieci.

Oba modele: OSI i TCP/IP mają wiele cech wspólnych. W obu przypadkach mamy koncepcje stosów niezależnych protokołów o zbliżonych funkcjach. Protokoły transportowe TCP i TP4 gwarantują użytkownikom prawie identyczne możliwości, zapewniając wysoką jakość i integralność przekazu typu end-to-end. W obu architekturach warstwa transportowa wspomaga realizację różnorodnych aplikacji. Z kolei warstwy niższe odpowiadają za efektywne funkcjonowanie podsieci komunikacyjnej.

Różnice między ISO-OSI i TCP/IP, wynikające z filozofii funkcjonowania jak też metodologii tworzenia zestawów protokolarnych, są jednakże duże. W przypadku ISO-OSI najpierw powstał model architektury, z perfekcyjnie wręcz opracowanymi definicjami usług warstwowych, interfejsów programowych i sprzętowych czy też funkcji warstw, a następnie opracowane zostały same standardy protokolarkie. W TCP/IP kolejność była dokładnie odwrotna. Fakt ten w istotny sposób wpłynął również na ograniczenie „rozmiarów” architektury - zamkującą ją w stosie czterowarstwowym. Inną istotną różnicą, zauważalną w obu modelach jest, wspomniany już powyżej, zakres stosowania w sieci połączeniowego bądź bezpołączniowego trybu realizacji usług. W TCP/IP preferowany jest tryb bezpołączniowy zapewniający większą efektywność i elastyczność pracy, szczególnie w przypadku sieci o wysokiej jakości i niezawodności.

W chwili obecnej również i sieci firmowe, takie jak SNA czy DECnet, są zdedykowane mniej popularne niż sieci publiczne, a szczególnie Internet.

W dziedzinie standardów i technologii sieciowych nic nie jest jednakże statyczne. Coraz to nowe rozwiązania zastępują stare i mniej efektywne, a strategie migracji protokołów i architektur sieciowych wymuszają w znacznej mierze użytkownicy usług sieciowych.

*Nie ulega wątpliwości, że w najbliższej przyszłości wspólnie będą obok siebie różnorodne architektury implementowane w różnych środowiskach, a znacząca część uwagi projektantów sprzętu i oprogramowania skierowana zostanie na opracowanie urządzeń, pozwalających na szybką konwersję aplikacji i protokołów funkcjonujących w odmiennych architekturach sieciowych.*

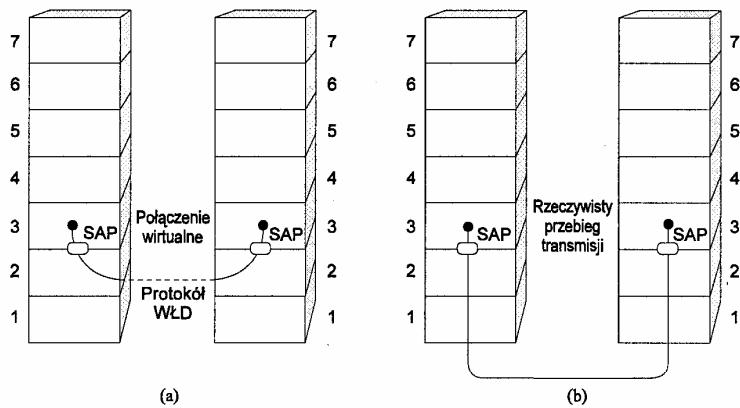
W opisie architektur zawartym w rozdziale 1, pominęliśmy model ATM. Model ten jednakże dość istotnie odbiega zarówno funkcjonalnie jak i koncepcyjnie od typowych architektur sieci pakietowych, jakimi są TCP/IP, ISO-OSI, SNA czy DNA. ATM jest koncepcją stworzoną głównie przez „lobby telefoniczne”, skupione wokół ATM-Forum. Sieć i architektura ATM wykorzystuje ideę komutacji krótkich pakietów, realizowaną w połączeniach wirtualnych. W powiązaniu z ogromnymi szybkościami przełączania w komutatorach ATM oraz dużymi przepustowościami systemów transmisyjnych, systemy ATM (B-ISDN ATM) oferują możliwość obsługi różnych typów ruchu, w tym świadczenia usług multimedialnych, z zagwarantowaniem ich pożądanej jakości oraz zapewnieniem skalowalności udostępnianych użytkownikowi zasobów sieci. Podobnie jak opracowane wcześniej standardy komunikacyjne X25, Frame Relay czy ISDN, standard ATM nie definiuje jednak pełnej architektury warstwowej, koncentrując się na opisie jedynie trzech warstw. Cechą charakterystyczną modelu ATM jest też jego „trójwymiarowość”. Obok warstw fizycznej, ATM i adaptacji, odpowiedzialnych za przekształcanie danych i ich pośrednictwo w transporcie z warstw wyższych do systemu transmisyjnego, w modelu wyróżniono tzw. płaszczyzny użytkownika i sterującą, a także płaszczyzny zarządzania warstwami i siecią. Problemom związanym z organizacją modelu B-ISDN ATM oraz perspektywom rozwoju ATM poświęcimy 7 rozdział książki.

## 2 Warstwa łącza danych - podstawowe funkcje i usługi

Z analizy pracy sieci, szczególnie sieci LAN, wynika kluczowe znaczenie warstwy łącza danych dla efektywnego funkcjonowania sieci komputerowych.

Warstwa łącza danych (WŁD) ma do spełnienia wiele specyficznych i ważnych funkcji. Funkcje te obejmują:

- zapewnienie właściwie zdefiniowanego styku z warstwą sieciową oraz świadczenie usług transportowych dla tej warstwy,
- określenie zasad grupowania w ramki bitów odbieranych z warstwy fizycznej oraz sposobu tworzenia ramek przy ich nadawaniu,
- nadzór nad poprawnością transmisji ramek przesyłanych przez zaszumione kanały cyfrowe,
- sterowanie przepływem ramek, w celu zapobiegania zalewaniu stacji odbiorczej nadmierną liczbą ramek nadawanych,
- zarządzanie dostępem do kanału.



Rys. 2.1. Ilustracja przepływu danych między obiektaми WS  
(a) wirtualnego, (b) rzeczywistego

Mówiąc o usługach świadczonych przez WŁD warstwom wyższym mamy na uwadze pośrednictwo w przekazie danych z warstwy sieciowej (WŚ) w jednym komputerze do warstwy sieciowej w innym komputerze, polegające na nawiązaniu wirtualnego połączenia obiektów warstwy WŁD we współpracujących stacjach/węzłach sieci. Zgodnie z koncepcją funkcjonowania architektur wars-

twoowych rzeczywista transmisja przebiega poprzez warstwy fizyczne i medium komunikacyjne, tj. w sposób pokazany na rysunku 2.1.

*WŁD jest zwykle projektowana z myślą o możliwości oferowania warstwie sieciowej różnych typów usług.* Usługi przekazu danych realizowane przez WŁD w sieciach komputerowych mogą być istotnie różne. Są one często określane mianem typów połączeń logicznych lub też trybów pracy sieci. Zgodnie z koncepcją modelu ISO OSI w warstwie łącza danych definiowane są trzy typy usług:

- usługa bezpołączniowa niepotwierdzana (ang. *connectionless unacknowledged service*); tzw. niepewny bezpołączniowy tryb pracy,
- usługa bezpołączniowa potwierdzana (ang. *connectionless acknowledged service*); tzw. pewny bezpołączniowy tryb pracy,
- usługa połączniowa (ang. *connection-oriented service*); tzw. połączniowy, lub połączniowo-zorientowany tryb pracy.

Usługi bezpołączniowe nie przewidują faz zestawiania oraz rozłączania w procesie wymiany informacji między obiektami WŁD. W przypadku usługi niepotwierdzanej, utracona ramka może być wykryta jedynie przez warstwę wyższą (np. WŚ lub WT). Ten typ usługi zalecany jest do obsługi zgłoszeń wymagających przetwarzania on-line w sieciach z kanałami fizycznymi wysokiej jakości. Należy tutaj podkreślić, że wiele sieci typu LAN i MAN realizuje ten typ usługi. Najbardziej skomplikowanym typem usług jest usługa zorientowana połączniowo. W tym przypadku przewiduje się zestawienie połączenia logicznego między obiektami WŁD komunikującymi się komputerów, przed każdym przekazem danych. Ramki przesyłane w fazie korespondencji są wówczas numerowane, a protokół WŁD gwarantuje odbiór każdej wyekspediowanej ramki. Ten rodzaj pracy WŁD jest powszechnie stosowany w sieciach rozległych WAN z tzw. transmisją typu punkt-punkt. Prawidłowa współpraca warstw poprzez styl programowy oraz poprawna realizacja logicznego przekazu danych przez WŁD wymaga zdefiniowania i właściwego realizowania sekwencji operacji podstawowych (por. rys.1.6).

W modelu ISO każde połączenie typu punkt-punkt, zapewniające dwukierunkowy wirtualny „przekaz” bitów realizowany przez warstwę fizyczną, ma na obu swoich końcach moduły oprogramowania WŁD. Ich zadaniem jest przekształcenie niepewnego przekazu bitów warstwy pierwszej, w wirtualne połączenie umożliwiające bezbłędną dwukierunkową transmisję pakietów. *Komunikacja pomiędzy obiektami WŁD realizowana jest przy tym asynchronicznie. Oznacza to w szczególności przypadkowy przedział czasu pomiędzy chwilą wprowadzenia pakietu do warstwy WŁD w jednej stacji, a chwilą jego wprowadzenia z tej warstwy w innej stacji. Przypadkowość ta może być wynikiem błędów w kanale fizycznym i koniecznych retransmisji ramek przez WŁD, jak też losowej długości pakietów. Również odstępy czasu pomiędzy momentami wprowadzania kolejnych pakietów do warstwy WŁD są przypadkowe. Może to*

wynikać zarówno z faktu, że warstwy wyższe (sieciowa, transportowa) nie mają pakietów do przesyłania bądź też z chwilowego przepelnienia buforów odbiorczych WŁD.

W celu świadczenia usług warstwie sieciowej WŁD musi korzystać z usług warstwy fizycznej (WF) - transmitującej strumień bitów. Aby przekaz bitów realizowany był efektywnie warstwa WŁD powinna w sposób jednoznaczny określać i identyfikować początek i koniec ramek. Z tego względu *proces ramkowania* (ang. framing) jest niezmiernie ważny. W najczęściej implementowanych rozwiązańach protokolarnych *do określenia początku i końca ramki stosuje się znaki początku i końca ramki - w protokołach zorientowanych znakowo - lub ciągi bitów stanowiące flagi początku i końca ramki - dla protokołów zorientowanych bitowo* (por. HDLC, SDLC, LAP-B, protokoły serii IEEE 802). W obu rozwiązaniach w celu uniknięcia błędnych interpretacji znaków lub bitów odpowiadających sekwencjom początku lub końca ramki pojawiającym się wewnątrz ramki stosowane jest *dodawanie znaków lub bitów nadmiarowych* (ang. stuffing). Bity te lub znaki są następnie usuwane w stacji odbiorczej. Stuffing nie jest stosowany w sieciach LAN.

Oprogramowanie WŁD ma również za zadanie tworzenie nagłówka czyli części organizacyjno-sterującej ramki. Część bitów nagłówka stanowią nadmiarowe bity kontrolne, pozwalające na *detekcję lub korekcję* błędów wnoszonych przez zaszumiony kanał cyfrowy (modem - kanał fizyczny - modem). Do zabezpieczenia transmisji przed błędami stosowane są głównie *blokowe kody liniowe*, a wśród nich *kody cykliczne*. W cyfrowych systemach telekomunikacyjnych coraz częściej znajdują też zastosowanie kody splotowe. W przypadku wykrycia błędów lub stwierdzenia utraty ramki realizowane są w warstwie WŁD *algorytmy retransmisji* błędnych lub straconych ramek. Algorytmy te mają charakter procedur rozproszonych realizowanych przez połączone logicznie moduły WŁD.

W zasadzie warstwa 2 (WŁD) w stacji odbiorczej wprowadza pakietы do warstwy sieciowej zgodnie z kolejnością ich wprowadzania do modułu WŁD w stacji nadawczej, jednakże nie wszystkie protokoły sterowania przepływem pakietów pomiędzy obiektami WŁD gwarantują tę własność.

Powyższe uwagi dotyczące współpracy modułów WŁD odnoszą się przede wszystkim do transmisji typu punkt-punkt. Transmisja taka ma miejsce w większości rozległych sieci komputerowych. Oznacza to w praktyce, że sygnały odbierane z kanału fizycznego stanowią zaszumioną replikę sygnałów nadawanych przez dokładnie jedną stację.

*W sieciach z medium „propagacyjnym” możliwa jest realizacja wielodostępu do wspólnego kanalu.* Odbierane przez stację sygnały mogą stanowić wówczas superpozycję sygnałów nadawanych przez stacje oraz szumu addytywnego. W systemach takich transmisje realizowane przez jedną ze stacji są słyszane przez wiele innych lub nawet wszystkie aktywne stacje sieci. Mówimy wówczas o transmisji rozsiewczej lub propagacyjnej typu punkt-wielopunkt (tj. kierowanej

## 2.1 Metody sterowania przepływem ramek w WŁD i ocena ich jakości

do wielu punktów). Sytuacje takie mają miejsce np. w komunikacji satelitarnej, radiowej jak też w sieciach z kablami koncentrycznymi (współosiowymi), światłowodowymi bądź wykorzystującymi łączą telefoniczne z wieloma odczepami (układami stykowymi).

Konstrukcja warstwy WŁD w sieciach z medium propagacyjnym różni się nieco od przyjętej dla sieci z połączaniami typu punkt-punkt. Zasadnicza różnica polega na rozbiciu tej warstwy na dwie podwarstwy: podwarstwę kanału logicznego (ang. Logical Link Control) oraz podwarstwę dostępu do medium (ang. Media Access Control). Ponadto w sieciach z medium propagacyjnym zacięta się granica pomiędzy podwarstwą MAC i warstwą fizyczną. Należy jednakże podkreślić, że bez względu na typ sieci podstawowe funkcje realizowane przez warstwę WŁD jako całość nie ulegają zmianie. Ma jedynie miejsce dalsza strukturalizacja oprogramowania i wyposażenia sprzętowego tej warstwy, głównie w odniesieniu do sieci MAN i LAN. Wydzielenie w tych sieciach zagadnienia zarządzania dostępem do medium od problemów świadczenia usług warstwom wyższym bądź sterowania przepływem ramek ma swoje odbicie w specyfice realizowanych protokołów komunikacyjnych.

W kolejnych rozdziałach pracy skoncentrujemy się na wybranych zagadnieniach funkcjonowania warstwy WŁD w sieciach WAN i LAN (ewentualnie MAN). Przedmiotem naszego zainteresowania będą problemy realizacji dostępu do medium oraz związane z nimi zagadnienia tworzenia ramek i sterowania ich przepływem.

Podrozdziały 2.1 i 2.2 zostaną poświęcone omówieniu ogólnych zasad sterowania przepływem ramek w sieciach teleinformatycznych oraz klasyfikacji metod dostępu do medium. Procedury protokolarkie odnoszące się do zarządzania dostępem i przekazem danych w sieciach lokalnych i rozległych będą szczegółowo omówione w następnych rozdziałach książki.

Czytelnika zainteresowanego innymi zagadnieniami, dotyczącymi na przykład stosowanych w sieciach komputerowych kodowych metod zabezpieczenia transmisji przed błędami, realizowanych na poziomie warstwy drugiej, odsyłamy do bogatej literatury.

### 2.1 Metody sterowania przepływem ramek w WŁD i ocena ich jakości

*Jedną z podstawowych funkcji WŁD, a także warstwy transportowej, jest sterowanie przepływem ramek.* W odbieranych przez stacje ramkach mogą pojawiać się błędy. W celu poprawnego dostarczenia ramek do stacji docelowej (ujścia) i zapewnienia tym samym integralności przesyłanych wiadomości stosowane są różne metody organizacji transmisji ramek. Metody te generalnie polegają na ponownej retransmisji wybranych ramek (co najmniej tych, które uległy uszkodzeniu) między określonymi (sąsiednimi, końcowymi) stacjami

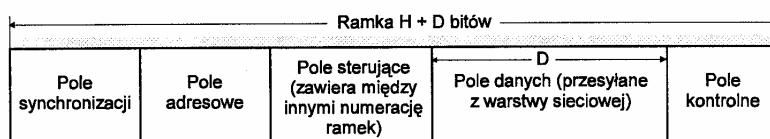
sieci. **Sterowanie przepływem ramek w sieci powinno być tak zorganizowane, aby nie dopuścić do zalewania stacji-adresata ramkami, przeciążenia i zakleszczenia pewnych węzłów sieci czy też nieograniczonego w czasie krążenia ramek po sieci.** Z drugiej strony **mechanizm wprowadzania nowych ramek do sieci powinien zapewnić efektywne wykorzystanie jej zasobów komunikacyjnych.** Oznacza to, że intensywność napływu nowych ramek powinna być możliwie duża i dostosowana do przepływności kanałów i/lub węzłów sieci.

Opisane w dalszej części tego rozdziału algorytmy sterowania przepływem znajdują zastosowanie głównie w sieciach WAN. Odnoszą się one bowiem do przypadku, gdy WŁD (bądź warstwa transportowa WT) realizuje usługi połączeniowe.

### 2.1.1 Charakterystyka ogólna algorytmów ARQ

**Protokoły warstwy łącza danych (PWŁD) zbudowane są z szeregu procedur umożliwiających wymianę informacji między komunikującymi się stacjami.** Jak wspominaliśmy wcześniej **komunikacja ta jest w zasadzie asynchroniczna.** Tym samym w celu prawidłowego przekazu danych ramki informacyjne bądź kontrolno-sterujące muszą przenosić informację służącą celom synchronizacji. Wzorcowe ciągi lub sekwencje znaków synchronizacji stanowią zwykle pole poczynające ramkę. Ramki odbierane z błędami muszą być powtarzane. Informacje o poprawnym lub błędny przekazie danych przekazywane są stronie nadawczej w wyniku realizacji stosownych procedur powiadamiania. **Zagadnienia wykrywania błędów, przesyłania powiadomień i odtwarzania utraconych danych stanowią przy tym część ogólnego problemu zapewnienia integralności danych w architekturach warstwowych. Integralność ta wymaga by ramki przesyłane pomiędzy stacjami były numerowane, w celu umożliwienia dostarczania ich warstwom wyższym we właściwej kolejności.**

Aby zrealizować powyższe funkcje ramki transmitowane między stacjami posiadają specjalne pola zabezpieczeń kodowych oraz pola kontrolno-sterujące zawierające w szczególności numery przesyłanych wiadomości. Dane zawarte w pakiecie przekazywanym do WŁD z warstwy WS wraz z polami organizacyjno-sterującymi generowanymi przez WŁD tworzą ramkę (w szczególności ramkę informacyjną). Przykładową strukturę hipotetycznej ramki informacyjnej ilustruje rysunek 2.2.



Rys. 2.2. Struktura przykładowej ramki informacyjnej WŁD

W literaturze opisano wiele procedur wykrywania i korekcji błędów jak też odtwarzania zniekształconych bądź utraconych ramek. W sieciach teleinformatycznych powszechnie zastosowanie znalazła jednakże technika nazywana ogólnie metodą ARQ (ang. Automatic Repeat reQuest), wiążąca wykrywanie błędów z automatyczną retransmisją ramek. Możliwe są przy tym różne wersje procedury ARQ. W rozwiązaniach tych przyjmuje się, że każda poprawnie odbiorana ramka może być potwierdzona indywidualnie, specjalną ramką powiadomienia pozytywnego (ACK), bądź też potwierdzenie może być wtrącone jako część pola kontrolno-sterującego ramki informacyjnej bądź sterującej przesyłanej w kierunku przeciwnym. Informacje o błędnie przesłanych ramkach mogą być przekazywane stacji źródłowej w postaci powiadomień negatywnych, tj. specjalnych ramek NAK. Gdy ramki NAK nie są w danym protokole stosowane, lub gdy mogą one ulegać zniekształceniom, dużym opóźnieniem bądź zakleszczeniom w transmisji (ang. deadlock), wówczas przeciwidałmy temu stosując mechanizm upływu czasu (ang. time-out); oznacza to, że w przypadku braku odbioru ramki ACK lub NAK w określonym przedziale czasu nadajnik automatycznie retransmituje daną ramkę. Ażeby zrealizować procedurę time-out-u kopie ramek wysyłanych przez stację nadawczą muszą być buforowane do chwili odbioru powiadomienia ACK.

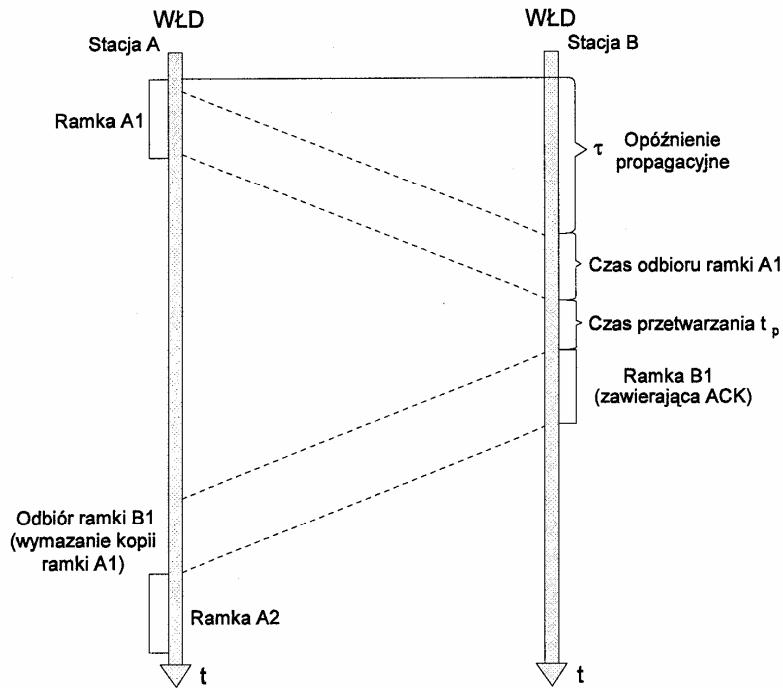
Istnieje szereg sposobów realizacji procesu transmisji/retransmisji ramek w zależności od napływu ACK/NAK. Najpowszechniejsze zastosowanie znajdują algorytmy typu „wyślij i czekaj” (ang. Stop-And-Wait - SAW) oraz algorytmy okienkowe typu Go-Back-N (GBN) i z selektywną retransmisją (ang. Selective Repeat).

### 2.1.2 Protokół Stop-And-Wait (SAW)

Zgodnie z protokołem SAW nadajnik przesyła przez kanał tylko jedną ramkę informacyjną, a następnie czeka na odbiór ACK/NAK. Jeżeli żadna z tych ramek nie napłynie w okresie time-out-u to ramka informacyjna musi być retransmitowana. Jedynie odbiór ACK pozwala na wymazanie kopii ramki informacyjnej przechowywanej w buforze stacji źródłowej. Praca stacji realizowana zgodnie z protokołem SAW w połączeniu punkt-punkt przedstawiona jest na rysunku 2.3.

W poprzednim paragrafie wspomnieliśmy, że w celu zapewnienia właściwej kolejności przesyłania ramek informacyjnych (a właściwie zawartości ich pól danych) do warstwy sieciowej muszą być one numerowane. W przypadku protokołu SAW z powiadaniem pozytywnym do numerowania ramek wystarczy użycie pojedynczego bitu (0 lub 1). W każdej chwili odbiornik oczekuje bowiem na ramkę o jednoznacznie określonym kolejnym numerze, a napływaną ramkę zawierającą niewłaściwy numer jest traktowana jako duplikat i odrzucana (nie jest ona przesyłana do warstwy sieciowej). Gdy napływaną ramkę ma numer zgodny z numerem oczekiwany, wówczas jej zawartość jest przesyłana do warstwy sieciowej, a numer kolejnej oczekiwanej ramki jest zwiększany zgodnie

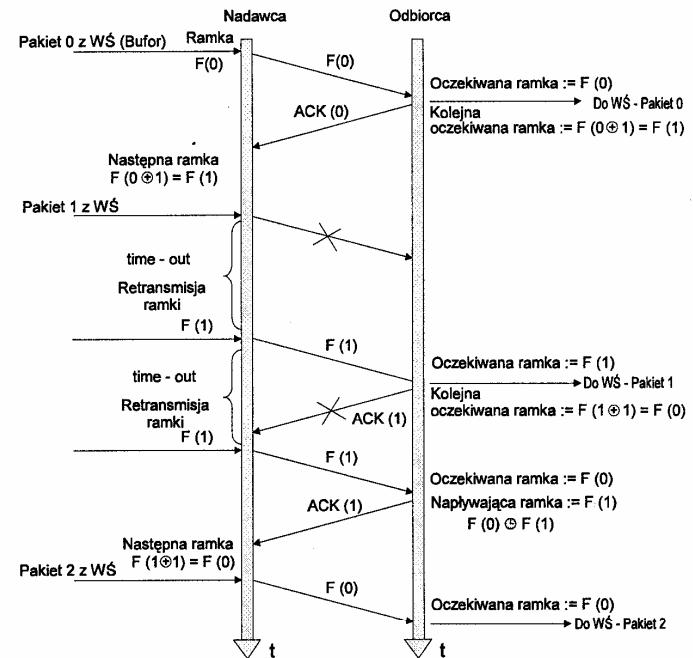
z operacją dodawania modulo 2. Przykład półdupleksowej transmisji ramek informacyjnych ilustruje rysunek 2.4.



Rys. 2.3. Ilustracja funkcjonowania protokołu SAW

Należy tutaj zwrócić uwagę na fakt, że protokół *SAW* został zaprojektowany przede wszystkim z myślą o nadzorowaniu przepływu informacji w połączeniu **półdupleksowym**, czyli przy naprzemiennej pracy stacji. Protokół ten może być też stosowany w pełniodupleksowej wymianie informacji. Jednakże z uwagi na konieczność oczekiwania na potwierdzenie każdej ramki informacyjnej wydajność tego protokołu nie jest zwykle zadowalająca. Ogólnie możemy stwierdzić, że stosowanie protokołu SAW (zarówno w połączeniu półdupleksowym jak i dupleksowym) staje się nieefektywne, gdy opóźnienia propagacyjne w łączach są porównywalne z czasami transmisji ramek informacyjnych. Jaskrawym przykładem złego zastosowania protokołu stop-and-wait może być jego użycie do przesyłania krótkich ramek (o czasach transmisji np. rzędu milisekund) przez łączę satelitarne wnoszące opóźnienia rzędu setek milisekund. Zagadnienie oceny jakości protokołu stop-and-wait będzie przedmiotem naszych dalszych rozważań.

### 2.1.3 Protokoły okienkowe



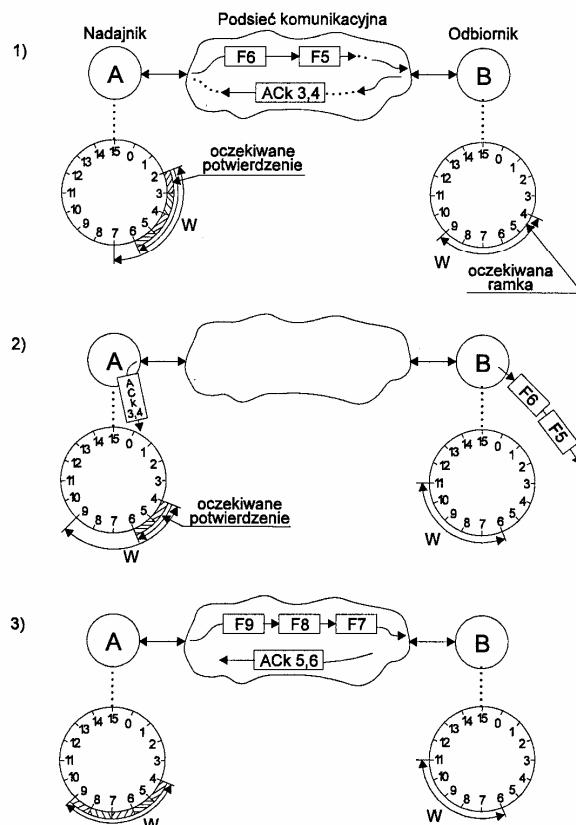
Rys. 2.4. Ilustracja półdupleksowej transmisji ramek w protokole SAW z powiadomieniem pozytywnym i retransmisjami

### 2.1.3 Protokoły okienkowe

Cechą charakterystyczną wszystkich protokołów okienkowych jest możliwość nadawania pewnej liczby  $N > 1$  ramek do chwili wstrzymania transmisji i oczekiwania na odbiór powiadomień ACK o najwcześniej przesłanych ramkach.

We wszystkich protokołach z tzw. przesuwającym się oknem (bądź okienkiem) (ang. *sliding window protocols*), każda nadawana rama informacyjna jest numerowana od 0 do pewnej wartości maksymalnej  $S_{\max}$  (ang. *maximum sequence number*). Wartość  $S_{\max}$  jest przy tym równa  $2^n - 1$ , gdzie n jest długością ciągu binarnego, stanowiącego fragment jednego z pól sterujących ramki. Charakterystyczną własnością protokołów okienkowych jest *utrzymywanie przez nadawcę listy kolejnych numerów ramek wysłanych przez stację*. Zgodnie ze stosowaną wówczas terminologią *ramki te opisują tzw. okienko (okno) nadawcze*. Podobnie *odbiorca utrzymuje również pewną listę numerów ramek, określającą mianem okienka odbiorczego*, które może on zaakceptować w przypadku odbioru tych ramek. Kolejne numery ramek w okienku nadawczym reprezentują przy tym ramki wysłane, lecz jeszcze nie powiadomione pozytywnie.

Każdorazowo, gdy z warstwy sieciowej napływa do warstwy WŁD pakiet, tworzona jest ramka, której nadawany jest najwyższy kolejny numer. Po transmisji ramki okienko nadawcze jest powiększane o jeden. Gdy do stacji napływa powiadomienie ACK dotyczące ramki o najniższym numerze, wówczas kopia tej ramki jest usuwana z bufora stacji, a dolny skraj okienka nadawczego jest przesuwany o jeden (szerokość okienka maleje o jeden). Tym samym okienko nadawcze w sposób ciągły utrzymuje listę niepotwierdzonych ramek (modyfikując ją dynamicznie). Zauważmy przy tym, że jeżeli maksymalny wymiar okienka wynosiłby  $W_{\max}$ , wówczas stacja nadawcza musiała być wyposażona w  $W_{\max}$  buforów ramek. W trakcie wymiany korespondencji mamy zwykle do czynienia z sytuacją, gdy aktualna szerokość (otwarcie) okienka  $W$  jest mniejsza od jego szerokości maksymalnej  $W \leq W_{\max}$ .



Rys. 2.5. Ilustracja zasady pracy protokołu okienkowego dla  $S_{\max}=15$ ,  $n=4$  i  $W_n=W_0=5$

**Okno odbiorcze w WŁD reprezentuje ramki, które stacja może zaakceptować. Każda ramka nie „wpadająca” do okienka, tj. o numerze innym niż wynikający z numeracji w okienku, jest przez protokół stacji odbiorczej dyskwalifikowana i niszczona.** W przypadku odbioru ramki o numerze zgodnym ze skrajnym - najniższym - numerem okienka, jest ona akceptowana, a zawartość tej ramki zostaje przesłana do warstwy WS. Generowane jest też powiadomienie pozytywne, przesypane zwrotnie jako niezależna ramka ACK lub dołączane do ramki informacyjnej, a okienko odbiorcze stacji przesuwa się o jedną pozycję. Szerokość okienka odbiorczego jest przy tym stała. Zasadę pracy protokołu okienkowego dla  $n = 4$  ( $S_{\max} = 15$ ) oraz szerokości okienek: nadawczego ( $W_N$ ) i odbiorczego ( $W_O$ ) równych 5 ilustruje przykład podany na rysunku 2.5.

Wśród protokołów okienkowych najpowszechniejsze zastosowanie znajdują algorytmy Go-Back-N (GBN) i z Selektynową Retransmisją (SR)

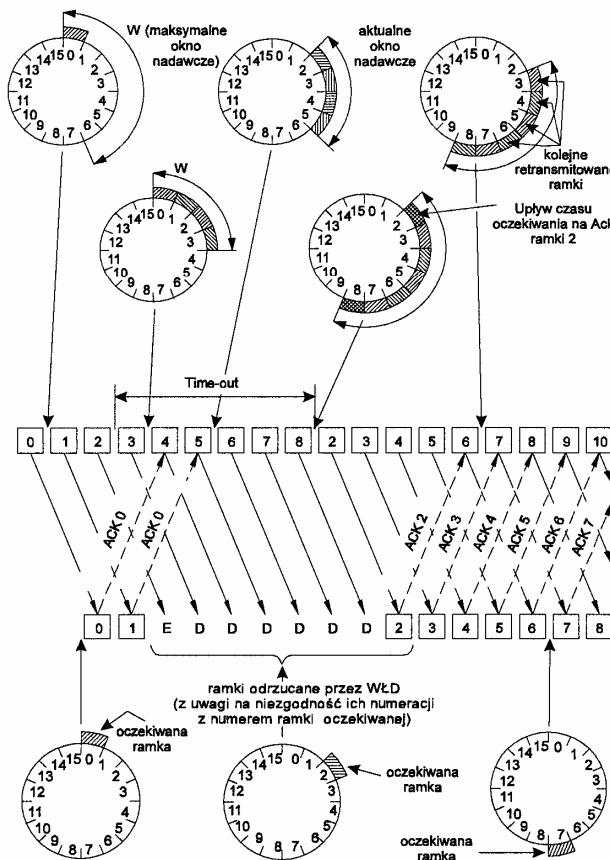
### 2.1.3.1 Protokół Go-Back-N (GBN)

W przypadku protokołu GBN zakładamy, że okienka nadawcze i odbiorcze mają różne wymiary, przy czym  $W_N \geq 1$ , a  $W_O = 1$ . Oznacza to, że po stronie odbiorczej zaakceptowana może być jedynie ta ramka, której numer odpowiada dokładnie jednemu numerowi oczekiwaniu. Każda inna ramka docierająca na stronę odbiorczą jest niszczona.

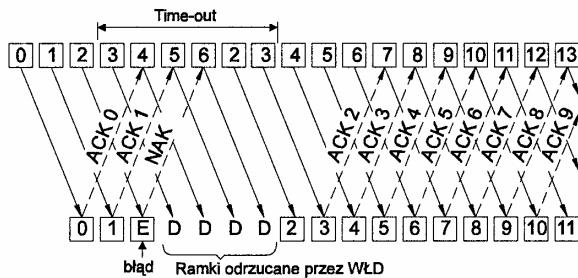
Podobnie jak w przypadku algorytmu SAW w momencie wysłania ramki uruchamiany jest przypisany jej zegar odliczający czas oczekiwania na nadanie powiadomienia ACK (time-out). Brak powiadomienia w przedziale time-out-u oznacza konieczność retransmisji ramki.

Na rysunku 2.6 pokazana jest zasada pracy protokołu GBN w przypadku gdy:  $S_{\max} = 15$ ,  $W_N = 7$ ,  $W_O = 1$ , time-out=6 ramek informacyjnych, a w systemie przesylane są jedynie ramki ACK (ramek NAK nie stosujemy). Z rysunku 2.6 wynika, że po utracie ramki o numerze 2, wszystkie kolejne ramki docierające do stacji odbiorczej będą niszczone, gdyż ich numery nie pokrywają się z numerem ramki oczekiwanej (nie wpadają do okienka odbiorczego). Zatem ramki o numerach 2-8 nie będą potwierdzone. Po wyczerpaniu limitu ramek nadawczych, tj. maksymalnym otwarciu okienka nadawczego stacja wysyłająca ramki wykrywa jednocześnie time-out dla ramki 2.

Algorytm GBN, z uwagi na jednopakietowy bufor odbiorczy, zmusza stację nadawczą do retransmisji wszystkich ramek począwszy od numeru 2. Innymi słowy Go-Back-N oznacza konieczność cofnięcia się o  $N$  pozycji wstecz (w naszym przykładzie  $N$  odpowiada liczbie ramek równoważnej time-out-owi) i retransmisję wszystkich wysłanych wcześniej ramek. Zwróćmy przy tym uwagę na fakt, że w praktyce nie ma potrzeby potwierdzania wszystkich ramek. Jedno ACK może potwierdzać wszystkie ramki informacyjne o numerach niższych i równym numerowi danej ramki (przy założeniu, że wszystkie one były odebrane bezbłędnie). W przypadku zastosowania w systemie ramek NAK algorytm pracy stacji mógłby ulec pewnym zmianom, w zależności od wartości przyjętego w protokole time-out-u. Ilustruje to rysunek 2.7.



Rys. 2.6. Zasada pracy protokołu GBN

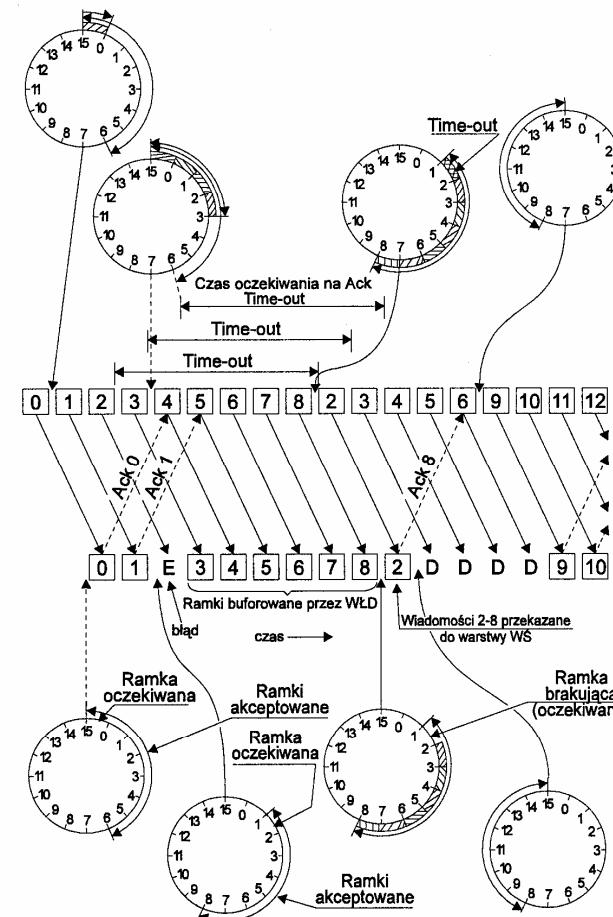


Rys. 2.7. Ilustracja protokołu GBN z pozytywnymi i negatywnymi powiadomieniami (ACK i NAK)

Należy podkreślić, że algorytm GBN jest stosowany w standardowych implementacjach protokołów warstwy WŁD omawianych w dalszej części książki.

### 2.1.3.2 Protokół z selektywną retransmisją (SR)

*Protokół z Selektyną Retransmisją posiada wbudowane procedury pozwalające na bardziej elastyczne reagowanie na błędy w transmisji ramek.* Zakładamy przy tym, że *oba okienka mają jednakowe wymiary*  $W_N = W_O = W$  *większe od 1*. Oznacza to, że pojemności buforów nadawczego i odbiorczego są takie same i umożliwiają przechowywanie do  $W$  ramek.



Rys. 2.8. Ilustracja pracy protokołu SR dla  $S_{max}=15$ ,  $W=7$  i Time-out =6

Ilustracja pracy protokołu SR przy założeniu, że  $S_{\max} = 15$ ,  $W = 7$ , time-out=6 ramek informacyjnych, a w systemie są przesyłane jedynie ramki ACK pokazana jest na rysunku 2.8.

Zgodnie z zasadą pracy protokołu ramki o numerach 3÷8 odbierane po błędnie odtworzonej ramce 2 nie są niszczone. Z uwagi na to, że ich numery mieszczą się w okienku odbiorczym, są one buforowane w warstwie WŁD stacji odbiorczej. Ich zawartości nie są jednakże przekazywane do warstwy sieciowej z uwagi na brak ramki 2. Pamiętamy, że WŁD winna dostarczać ramki do WS we właściwej kolejności. Po upływie time-out-u ramka 2 i kolejne są retransmitowane przez stację źródłową. W chwili zakończenia odbioru retransmitowanej ramki 2, stacja odbiorcza generuje powiadomienie grupowe (ACK(8)). Odbiór tego powiadomienia przez stację nadawczą przerywa realizowaną przez nią retransmisję ramek. Możemy więc mówić o selektywności retransmisji. Obie stacje modyfikują też swoje okienka. Stacja odbiorcza przesyła zawartość buforów - wypełnionych ramkami o numerach 2÷8 - do warstwy sieciowej i przesuwa okienko odbiorcze na ramki o numerach 9÷15. Z kolei stacja nadawcza po odbiorze ACK(8) przechodzi do nadawania ramek o numerach 9, 10 i kolejnych. Ramki informacyjne o numerach 3, 4, 5 i 6 docierające do stacji odbiorczej są przez nią traktowane jako duplikaty i są niszczone, gdyż nie odpowiadają one numerom zmodyfikowanego okienka odbiorczego.

Podobnie jak w protokole GBN wprowadzenie powiadomień negatywnych może przynieść pewną poprawę efektywności pracy protokołu, poprzez zwiększenie jego elastyczności.

Tabela 2.1. Porównanie przykładowych parametrów podstawowych protokołów ARQ

Protokół	Wymagana wielkość pamięci buforowej (w ramkach)		Konieczność odtwarzania kolejności napływających ramek	Złożoność algorytmu
	Stacja nadawcza	Stacja odbiorcza		
S-W	1	1	nie istnieje	mała
GBN	N	1	nie istnieje	średnia
SR	N	N	istnieje	duża

Pomimo lepszych parametrów jakościowych, protokół okienkowy z Selektynną Retransmisją ramek jest mniej popularny od GBN; wiąże się to częściowo z koniecznością wydzielenia większych pojemności pamięci buforowych w stacji odbiorczej (w porównaniu z GBN) (tab.2.1) oraz koniecznością realizacji przez ten protokół (SR) procedur porządkowania kolejności ramek przed ich przesłaniem do warstwy sieciowej. Przewiduje się jednakże, że zmiany zachodzące w technologii VLSI oraz w technikach programowania mogą spowodować szybkie zastąpienie protokołu GBN protokołem SR.

## 2.1.4 Ocena jakości protokołu SAW oraz protokołów okienkowych

By przybliżyć Czytelnikowi ocenę jakości funkcjonowania i użyteczności poszczególnych metod sterowania przepływem ramek dokonamy zgrubnej analizy zmian efektywności wykorzystania kanału, tj. maksymalnego znormalizowanego przepływu, definiowanego jako iloraz czasu zajętego przez pole danych ramki (lub ramek, w zależności od wersji protokołu) przesłanej (przesyłanych) w przedziale czasu upływającym od rozpoczęcia transmisji najwcześniejszej ramki do chwili otrzymania powiadomienia pozytywnego o tej ramce do długości tego przedziału.

Badając sprawność mechanizmów SAW, GBN i SR interesować nas będzie przypadek, gdy stacje pracują w stanie „nasycenia”, tj. z dużym obciążeniem, mając cały czas ramki gotowe do transmisji. Założymy też, że błędy w kanałach, będące przyczyną ewentualnych retransmisji ramek są niezależne. Tym samym otrzymane oszacowania przepływu ramek w kanale będą oszacowaniami od góry charakteryzującymi przypadek najgorszy.

Przy analizie przyjmiemy przy tym następujące oznaczenia:

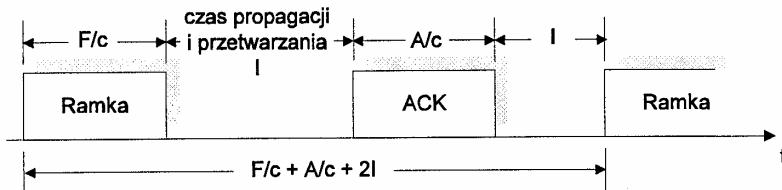
A	- liczba bitów w ramce ACK
D	- liczba bitów w ramce informacyjnej
H	- liczba bitów nagłówka ramki
F=H+D	- całkowita długość ramki (w bitach)
c	- szybkość transmisji w b/s
I	- czas propagacji ramki w kanale oraz przetwarzania ramki w stacji
T	- time-out (czas oczekiwania na odbiór ACK)
E	- prawdopodobieństwo błędu elementarnego
L	- prawdopodobieństwo utraty bądź zniekształcenia ramki informacyjnej lub ACK
P <sub>1</sub>	- prawdopodobieństwo utraty bądź zniekształcenia ramki informacyjnej
P <sub>2</sub>	- prawdopodobieństwo utraty bądź zniekształcenia ramki ACK
R	- średnia liczba retransmisji na jedną ramkę informacyjną
U	- wykorzystanie kanału (efektywne).

### 2.1.4.1 Jakość protokołu Stop-And-Wait

Rozważmy dwa przypadki związane z różną jakością kanału transmisyjnego. Analizować będziemy efektywność algorytmu SAW, gdy wykorzystywany jest idealny kanał bezszumowy, bądź kanał zaszumiony z błędami niezależnymi.

### A. Kanał bezszumowy

Przy wyznaczaniu współczynnika wykorzystania kanału U skorzystamy z interpretacji cyklu transmisyjnego podanej na rysunku 2.9.



Rys. 2.9. Ilustracja procesu transmisji ramek w SAW

Zgodnie z przyjętymi założeniami przepływ U może być wówczas wyrażony jako

$$U = \frac{D/c}{F/c + A/c + 2I} = \frac{D}{F + A + 2cI} .$$

### B. Kanał zaszumiony

W przypadku zniekształcenia lub utraty ramki nadawca będzie dokonywał jej retransmisji po upływie time-out-u T. Tym samym jedna nieudana transmisja angażuje  $F+cT$  bitów.

Jeżeli średnią liczbę retransmisji przypadającą na jedną udaną transmisję ramki oznaczmy przez R, to czas pomiędzy rozpoczęciem transmisji kolejnych ramek, opisany liczbą bitów, będzie równy:

$$R(F + cT) + F + A + 2cI .$$

Traktując zdarzenia utraty lub zniekształcenia ramek informacyjnych oraz ACK jako niezależne prawdopodobieństwo L utraty lub zniekształcenia jednej z tych ramek (co prowadzi do retransmisji) opisuje wzór

$$L = 1 - (1 - P_1)(1 - P_2) .$$

Przyjmując dalej, że proces retransmisji jest bezpamięciowy, tj. że warunki w kanale są stacjonarne, a reguła nadawczo-odbiorcza jest niezmienna w czasie, liczbę transmisji danej ramki możemy opisać rozkładem geometrycznym. Tym samym

$$P_r(k \text{ transmisji}) = L^{k-1}(1-L); \quad k = 1, 2, \dots$$

Średnia liczba retransmisji R (wartość średnia zmiennej losowej o rozkładzie geometrycznym) przyjmuje więc postać:

$$R = \frac{L}{1-L}$$

Wykorzystanie U kanału otrzymujemy zatem jako

$$U = \frac{D}{(L/1-L)(F+cT) + (F+A+2cI)} .$$

Jeżeli dodatkowo przyjmiemy minimalną wartość time-out-u (uwzględniającą podwojony czas propagacji w kanale i czasy przetwarzania w stacjach ( $2I$ ) oraz czas transmisji powiadomienia ACK ( $A/c$ )) równą

$$T \cong A/c + 2I ,$$

wtedy

$$U = \frac{D}{H+D} * (1-P_1)(1-P_2) * \frac{1}{1+cT/(H+D)} .$$

W wyrażeniu tym poszczególne czynniki reprezentują:

- (1) - wpływ nagłówka H ramki na zmniejszenie wykorzystania U,
- (2) - spadek wartości U na skutek błędów w transmisji,
- (3) - zmniejszenie wykorzystania spowodowane start-stopową (ang. stop-and-wait) pracą stacji.

W przypadku wykorzystania protokołu stop-and-wait do sterowania połączeniem punkt-punkt ważnym problemem staje się wybór optymalnej długości pola danych ramki. Jeżeli przyjmiemy, że:

- błędy w kanale są niezależne,
  - a
  - długość nagłówka ramki jest stała,
- to proste rozważania optymalizacyjne prowadzą do następującej wartości  $D_{opt}$  maksymalizującej U

$$D_{opt} = \frac{H+cT}{2} \left[ \sqrt{1 - 4 / [(H+cT) \ln(1-E)]} - 1 \right] .$$

W przypadku kanałów o wysokiej jakości, tj. takich dla których prawdopodobieństwo błędu elementarnego (elementowa stopa błędu) jest mniejsze od  $10^{-6}$  możemy przyjąć, że  $\ln(1-E) \cong -E$ .

Tym samym

$$D_{opt}|_{E \ll 1} \cong \sqrt{(H+cT)/E} .$$

W przypadku łącz y o  $E \cong 10^{-5}$  optymalna długość pola danych jest rzędu 1000 bitów, podczas gdy dla łącz satelitarnych o  $E \cong 10^{-7}$  mamy  $D_{opt}$  rzędu 20000 bitów (zwykle przyjmuje się, że w typowych łączach naziemnych  $E \cong 10^{-6}$ ).

Rozważmy, w formie prostego przykładu, wykorzystanie łącz y: satelitarnego i naziemnego łącz radioliniowego, pozwalających na transmisję z szybkością 50 kb/s. Przyjmijmy, że prawdopodobieństwa utraty lub zniekształcenia ramek są

pomijalnie małe. W obu przypadkach założymy też, że długości ramek są identyczne, a  $F \cong D$ , przy czym  $D = 10000$  bitów lub  $D = 1000$  bitów. Ponadto przyjmijmy, że długość łącza naziemnego jest równa 1000 km, a odległość satelity geostacjonarnego od każdej ze stacji naziemnych - około 40 tys. km.

Zakładając szybkość propagacji w obu przypadkach zbliżoną do prędkości światła, otrzymujemy następujące opóźnienia propagacyjne między stacjami

$$\text{– łącze naziemne: } I_n \cong \frac{1000}{300} 10^{-3} \text{ s} \cong 3.3 \text{ ms},$$

$$\text{– łącze satelitarne: } I_s \cong \frac{60000}{300} 10^{-3} \text{ s} \cong 270 \text{ ms}.$$

Przyjmując, że czasy przetwarzania ramek są małe w stosunku do  $I_n$  oraz  $I_s$ , a  $H \ll D$  wykorzystanie łączy w obu rozważanych przypadkach jest równe:

– dla łącza naziemnego:

$$U_n \cong 0.96 \text{ dla } D = 10000 \text{ bitów} \quad (96\%)$$

$$U_n \cong 0.75 \text{ dla } D = 1000 \text{ bitów} \quad (75\%)$$

– dla łącza satelitarnego:

$$U_s \cong 0.24 \text{ dla } D = 10000 \text{ bitów} \quad (24\%)$$

$$U_s \cong 0.036 \text{ dla } D = 1000 \text{ bitów} \quad (3.6\%)$$

Powyższe wyniki nie wymagają dodatkowego komentarza.

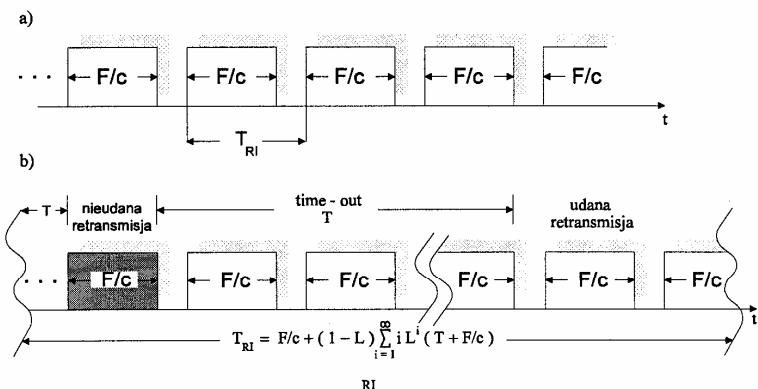
#### 2.1.4.2 Jakość protokołów okienkowych

Przedstawimy teraz uproszczoną analizę jakości protokołów okienkowych GBN i SR dla kanałów zaszumionych. Przyjmiemy przy tym oznaczenia identyczne jak przy analizie protokołu SAW.

##### Protokół GBN

W przypadku tego protokołu założymy, że zarówno szerokość okna nadawczego  $W_N$  jak i numeracja kolejnych ramek od 0 do  $S_{\max}$  są odpowiednio duże, tzn.  $W_N \geq 1 + 2cl/F$  (jest to przypadek tzw. szerokiego okna), pozwalając tym samym na ciągłą transmisję ramek informacyjnych; bez konieczności zatrzymywania pracy stacji i oczekiwania na odbiór ACK. Założymy też, że stacje mają zawsze ramki gotowe do przesłania. Przypomnijmy, że w metodzie GBN wszystkie ramki napływające po ramce odebranej z błędem muszą być retransmitowane po upływie time-out-u ( $T$ ). Tak więc minimalny czas między transmisjami wynosi  $F/c$ , a pojedynczy cykl oddzielający dwie kolejne re/transmisje tej samej ramki ma długość  $T+F/c$ . Tym samym średni czas transmisji ramki (prezentowany na rysunku 2.10), ma w przypadku zaszumionego kanału (i przy dopuszczeniu nieograniczonej liczby retransmisji ramek) postać:

$$T_{RI} = F/c + (1-L) \sum_{i=1}^{\infty} iL^i (T+F/c) = F/c + \frac{L}{1-L} (T+F/c)$$



Rys. 2.10. Ilustracja czasów  $T_{RI}$  udanych transmisji ramek w GBN (a) kanał bezszumowy, (b) kanał zaszumiony

Oznacza to, że zgodnie z algorytmem GBN wszystkie ramki przesyłane w okresie  $T_{RI}$  są retransmitowane.

Po prostych przekształceniach otrzymujemy następującą postać wyrażenia na wykorzystanie U kanału:

$$U = \frac{D/c}{T_{RI}} = \frac{D/c}{F/c + \frac{L}{1-L} (T+F/c)} = \frac{D}{H+D} * (1-L) * \frac{1}{1 + LcT/(H+D)}.$$

W przypadku kanału niezaszumionego (transmisje bezbłędne) wykorzystanie U jest oczywiście równe:

$$U = \frac{D}{H+D}.$$

Jeżeli, podobnie jak w przykładzie analizowanym poprzednio, dla algorytmu SAW, przyjmiemy, że do przekazu ramek o długości  $F=10000$  bitów, bądź 1000 bitów, przy czym  $F \cong D$ , wykorzystywane jest łącze satelitarne pozwalające na transmisję z szybkością 50 kb/s, to okaże się, że w przypadku kanału bezszumowego maksymalną efektywność  $U$ , bliską 1 (100%), uzyskamy przyjmując następujące szerokości okna nadawczego:

$$W_{N,\min} = 4 \quad (W_N \geq 3.7) \text{ dla } F \cong D = 10000 \text{ bitów},$$

$$W_{N,\min} = 37 \quad (W_N \geq 37) \text{ dla } F \cong D = 1000 \text{ bitów}.$$

Zakładając dalej użycie okna  $W_N = 4$  do sterowania przepływem ramek o długości 10000 bitów w kanale zaszumionym, w którym prawdopodobieństwo zwiększenia ramki F bądź powiadomienia ACK wynosi  $L=0.01$ , to wartość wykorzystania kanału będzie w przybliżeniu równa:

$$U \geq 0.96 \text{ (96%).}$$

Tym samym nawet retransmisje co setnej ramki nie spowodują istotnego pogorszenia efektywności algorytmu GBN, która to efektywność, przy przyjętych powyżej założeniach, około czterokrotnie przewyższa efektywność algorytmu SAW.

#### Protokół z Selektyną Retransmisią

Rozważmy tym razem dwa przypadki:

- (1) przypadek szerokiego (dużego) okna, gdy

$$W_N \geq 1 + 2cI / F$$

oraz

- (2) przypadek wąskiego (małego) okna, gdy

$$W_N < 1 + 2cI / F.$$

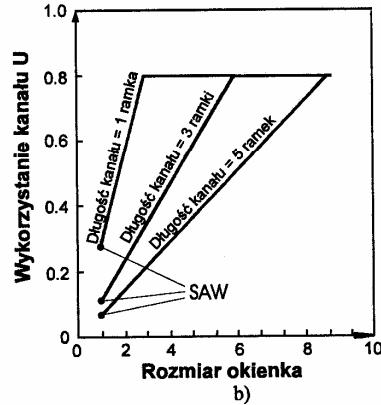
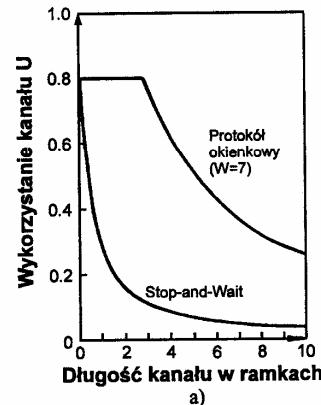
Zakładając selektywną retransmisję błędnie przesyłanych ramek (a nie jak w GBN całych serii ramek) średnia liczba transmisji przypadających na jedną ramkę wynosi  $1/(1-L)$ . Odbiór  $W_N$  bezbłędnych ramek wymaga więc średnio transmisji  $W_N/(1-L)$  ramek. Tym samym otrzymujemy:

- (1) dla szerokiego okna:

$$U = \frac{D}{H+D} * (1-L)$$

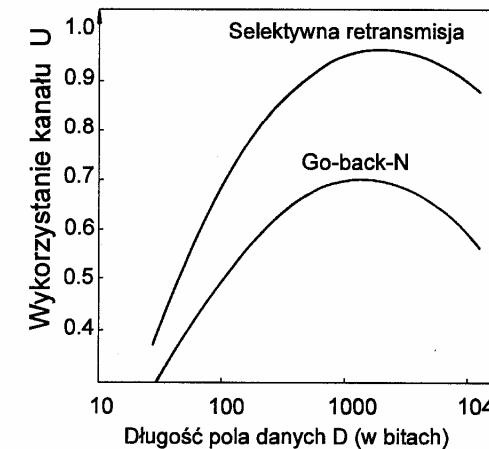
- (2) dla wąskiego okna:

$$U = \frac{D}{H+D} * (1-L) * \frac{W}{1 + 2cI / (H+D)}.$$

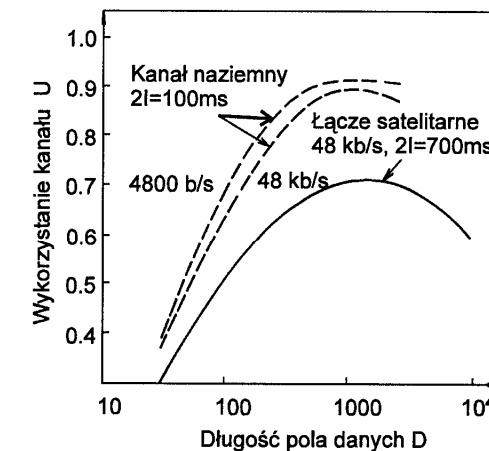


Rys. 2.11. Porównanie zmian wykorzystania kanału w systemach z protokołami SAW i SR w przypadku kanałów bezszumowych

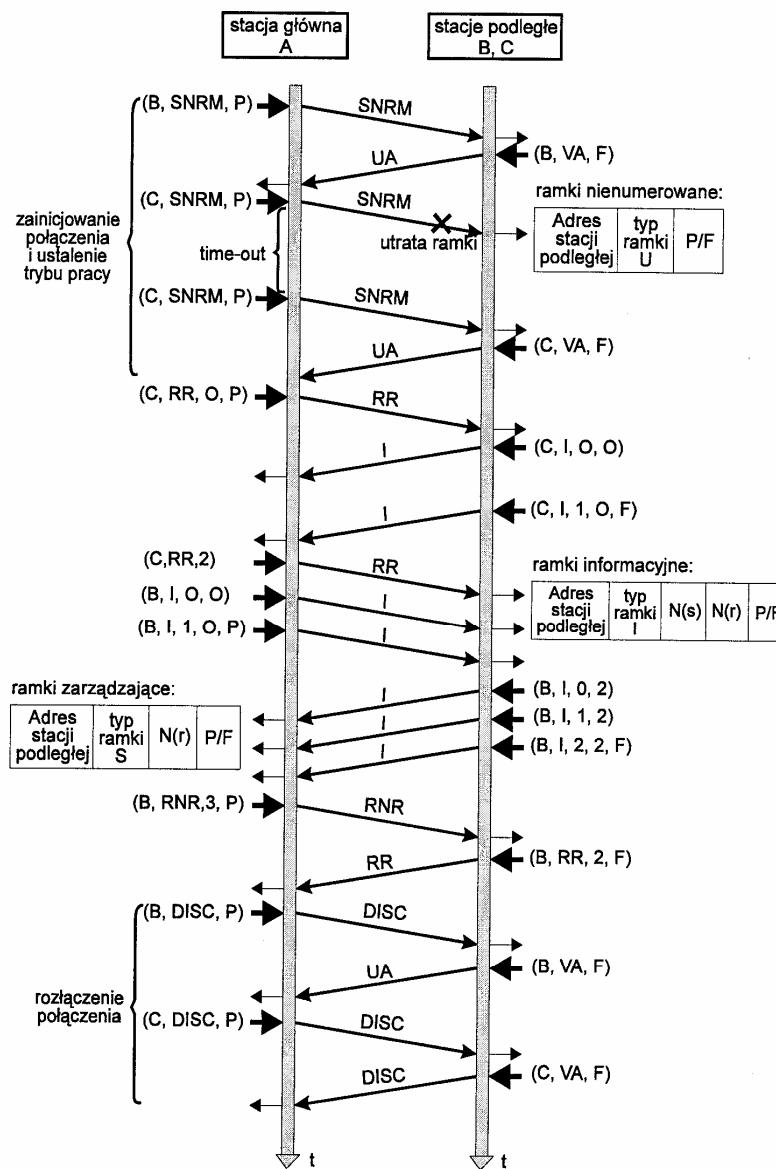
Porównanie jakości analizowanych protokołów przy zmianach opóźnień propagacyjnych (długości kanałów), szerokości okien oraz długości przesyłanych ramek przedstawiono na rysunkach od 2.11 do 2.14. Na rysunkach tych parametrami są szybkości transmisji oraz jakości kanałów.



Rys. 2.12. Wykorzystanie kanału satelitarnego w przypadku stosowania procedur z selektywną retransmisją (SR) i GBN dla  $c=48 \text{ kb/s}$ ,  $2I=700 \text{ msec}$ ,  $E=10^{-5}$ ,  $H=48 \text{ bitów}$



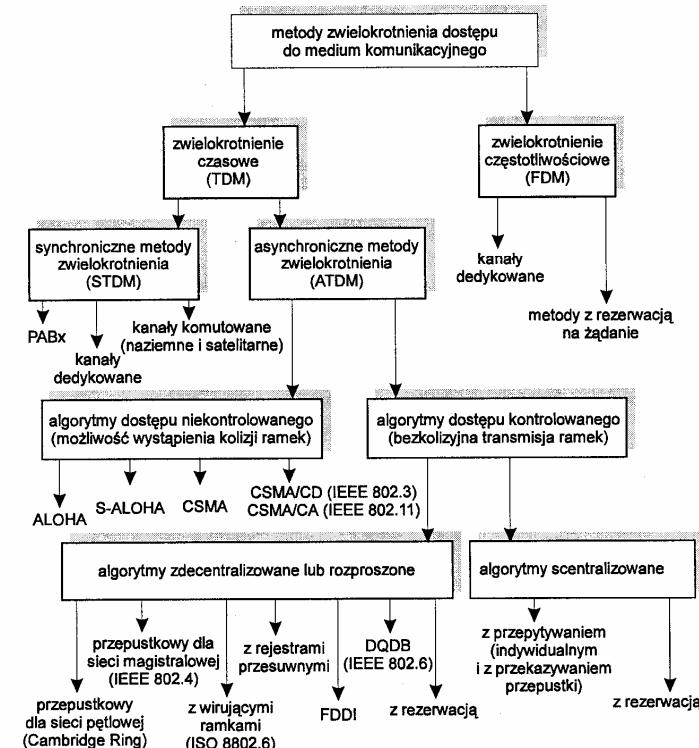
Rys. 2.13. Wykorzystanie kanału dla protokołu GBN w przypadku, gdy  $E=10^{-5}$ ,  $H=48 \text{ bitów}$



Rys. 2.14. Wykorzystanie kanału satelitarnego w funkcji zmiany stopy błędów E, D=1000 bitów, H=48 bitów

## 2.2 Ogólna charakterystyka metod arbitracji dostępu do medium komunikacyjnego - klasyfikacja protokołów podwarstwy MAC

Jedną z podstawowych funkcji warstw WŁD jest sterowanie dostępem do medium. W systemach z transmisją punkt-punkt zagadnienie to sprowadza się do określenia najkorzystniejszych i jednoznacznych warunków współpracy dwóch połączonych wzajemnie urządzeń. W sieciach ze wspólnym medium komunikacyjnym (określonym nierzaz mianem medium propagacyjnego) umożliwiającego transmisję rozgłoszeniową (nazywaną też wielopunktową) najważniejszym problemem staje się określenie zasad współużytkowania wspólnego medium.



Rys. 2.15. Klasyfikacja metod dostępu do medium komunikacyjnego

W większości funkcjonujących sieci teleinformatycznych media komunikacyjne (kanały fizyczne) dostępne dla stacji końcowych i/lub węzłowych oferują duże

przepustowości. Właściwe ich wykorzystanie jest możliwe poprzez zastosowanie technik zwielokrotnienia dostępu. Dominującą rolę odgrywają przy tym metody zwielokrotnienia czasowego (ang. *Time Division Multiplexing* - TDM) oraz częstotliwościowego (ang. *Frequency Division Multiplexing* - FDM). W ostatnim okresie coraz częściej stosuje się też kodowe metody zwielokrotnienia (ang. *Code Division Multiplexing* - CDM).

Rysunek 2.15 przedstawia propozycję klasyfikacji protokołów MAC (technik dostępu do podkanałów czasowych lub częstotliwościowych wydzielonych w medium wielodostępnym). We wszystkich przypadkach **wiele połączeń logicznych współużytkuje przepustowość określonego kanału fizycznego**. Realizacja połączeń z wykorzystaniem kanałów dedykowanych (np. dzierżawionych) bądź komutowanych, wydzielonych techniką FDM ma głównie miejsce w pakietowych sieciach rozległych (WAN) realizujących połączenia typu punkt-punkt, bądź też w tzw. szerokopasmowych - multimedialnych sieciach LAN. W dziedzinie czasu synchroniczne metody zwielokrotnienia dostępu TDM stosowane są zarówno w sieciach rozległych do wydzielania podkanałów łączących węzły sieci komunikacyjnej (w oparciu o technikę PCM) jak też w pracujących w oparciu o PCM instalacjach central lokalnych PABX realizujących komutację połączeń między abonentami lokalnymi.

**W przypadku sieci LAN stosowane w nich metody dostępu do medium związane są zwykle z realizacją asynchronicznego zwielokrotnienia czasowego.** Oznacza to, że stacjom nie są przydzielane w sposób sztywny powtarzające się szczeliny czasowe. Dostęp do kanału w systemie z asynchronicznym TDM może być w szczególności całkowicie przypadkowy, jak to ma miejsce w algorytmach ALOHA bądź S-ALOHA (ang. *Slotted ALOHA*). Oznacza to, że stacje dokonują prób dostępu w losowych chwilach czasu, lub w przypadkowo wybranych szczelinach i bez wzajemnej koordynacji, co może prowadzić do kolizji przesyłanych ramek informacyjnych. Popularnymi protokołami częściowo-kontrolowanego dostępu są algorytmy CSMA; wykorzystywane jako np. protokół podwarstwy MAC w amatorskich sieciach radiowych (jako część pakietu oprogramowania AX25), jak też CSMA/CD - będące standardem IEEE 802.3 dla przewodowych sieci LAN. W ostatnim okresie czasu opracowane zostały nowe standardy dla bezprzewodowych sieci LAN. Są to: IIIPERLAN (pilotowany przez ETSI) oraz IEEE 802.11. We wszystkich tych rozwiązaniach częściową eliminację kolizji zapewnia badanie stanu kanału przed każdą próbą re/transmisji ramki. Protokoły te będą omawiane w dalszej części książki. Metody kontrolowanego lub regulowanego dostępu dzielimy na zdecentralizowane (ewentualnie rozproszone) i scentralizowane. Do pierwszej grupy zaliczymy algorytmy z przekazywaniem znacznika - tokena, w tym: standardowy protokół tokenowy dla sieci magistralowej IEEE 802.4 oraz tokenowy protokół dostępu do sieci pętlowej IEEE 802.5, a ponadto algorytm z tzw. pierścieniem szczelinowym (ang. *Cambridge Ring lub Slotted Ring*) oraz protokół ANSI stosowany w światłowodowej sieci FDDI (ang. *Fiber Distributed Data Interface*). Do grupy protoko-

## 2.2 Ogólna charakterystyka metod arbitracji dostępu do medium komunikacyjnego...

łów o rozproszonym (zdecentralizowanym) algorytmie dostępu zaliczamy też metodę stosowaną w sieci pętlowej z rejestrami przesuwanymi oraz metody rezerwacji, w tym algorytm DQDB (ang. *Distributed Queue Dual Bus*) stosowany w standardzie IEEE 802.6 dla sieci MAN.

Warto tutaj zwrócić uwagę na fakt, że przykładowe algorytmy rywalizacyjnego dostępu, tj. ALOHA, S-ALOHA, CSMA, CSMA/CD są również algorytmami zdecentralizowanymi, podobnie jak reguły dostępu dla sieci pętlowych z wirującymi szczelinami (z pierścieniem szczelinowym) i rejestrami przesuwnymi. W literaturze wyróżnia się czasem metody zdecentralizowane i rozproszone jako dwie niezależne grupy algorytmów. Do pierwszej grupy zaliczamy te metody, w których dostęp wszystkich stacji realizowany jest każdorazowo na zasadach rywalizacji (prowadzi często do kolizji). Druga grupa obejmuje np. metody tokenowe (IEEE 802.4, 802.5), w których posiadacz tokena może przez określony czas przesyłać kolejne ramki bez konieczności rywalizacji o dostęp do medium.

Ostatnia grupa reguł prezentowanych na rysunku 2.15 i omawianych w niniejszej książce obejmuje realizowane w sposób scentralizowany przepytywanie (ang. *polling*), powszechnie stosowane w połączeniach wielopunktowych (por. też IEEE 802.12 - 100VGAnyLAN) oraz metody rezerwacji, wykorzystywane np. w systemach łączności osobistej i systemach satelitarnych VSAT. Istnienie w systemie satelitarnym naturalnego sprzężenia zwrotnego, zapewniającego przez fakt retransmisiji przez przekaźnik satelitarny do stacji naziemnych sygnałów nadawanych przez te stacje, pozwala na realizację systemu rozproszonego o cechach bardzo efektywnego systemu scentralizowanego.

Należy tutaj zwrócić uwagę na fakt, że większość z wymienionych powyżej algorytmów dostępu odnosi się do sieci z „propagacyjnym” (rozsiewczym) medium komunikacyjnym. Tym samym algorytmy te znajdują zastosowanie przede wszystkim w przewodowych bądź bezprzewodowych sieciach LAN i MAN oraz satelitarnych wersjach sieci WAN.

### 3 Protokoły warstwy łącza danych w sieciach rozległych WAN

**Rozległe sieci komputerowe** (ang. WAN - Wide Area Networks) możemy w sposób ogólny zdefiniować jako zbiory autonomicznych komputerów i urządzeń końcowych połączonych podsiecią komunikacyjną. Sieci te łączą komputery, urządzenia końcowe jak też sieci lokalne na poziomie połączeń krajowych bądź międzynarodowych. Najważniejsze standardy (zalecenia) odnoszące się do tych sieci dotyczą:

- a) mediów komunikacyjnych (modemy, łącza, itp.),
- b) styków sprzętowych (interfejsów fizycznych),
- c) protokołów warstwy łącza danych,
- d) architektur sieciowych.

Parametry charakteryzujące sieci WAN istotnie różnią się od parametrów bardzo popularnych sieci lokalnych. W szczególności:

- opóźnienia propagacyjne w sieciach WAN są dużo większe niż w sieciach LAN, a w przypadku wykorzystania łączy satelitarnych sięgają setek milisekund;
- prędkości transmisji są z reguły znacznie niższe od stosowanych w instalacjach lokalnych;
- dużo wyższe są częstości pojawiania się błędów, co sprawia, że procedury ich wykrywania i usuwania stają się niezbędne;
- w sieciach WAN wiele instytucji i organizacji ma wpływ na typy instalowanych urządzeń końcowych i komputerów, jak też stosowane w nich standardy protokolarne; podczas gdy sieci LAN są zwykle prywatne i administrowane przez jedną organizację;
- łącza transmisyjne w sieciach WAN są bardziej podatne na uszkodzenia, w związku z tym w sieciach tych uwzględnia się możliwości rekonfiguracji strukturalnej;
- sieci WAN to sieci z transmisją wieloetapową i z komutacją pakietów, zapewniające przekaz pakietów o różnych rozmiarach i w róŜnej kolejności; często dokonywana jest też konwersja protokołów;
- koszty korzystania z usług sieci WAN związane są zwykle z objętością przesyłanych wiadomości; podczas gdy w sieciach LAN są najczęściej stałe.

W odniesieniu do sieci WAN protokół WŁD warstwy łącza danych (zgodnie z architekturą ISO) stanowi zestaw zasad zapewniających uporządkowaną

wymianę informacji pomiędzy fizycznie połączonymi stacjami/węzłami sieci. Sieci komputerowe lat sześćdziesiątych korzystały powszechnie z opracowanego przez IBM i zorientowanego znakowo protokołu BISYNC (BSC). W połowie lat siedemdziesiątych firma DEC wprowadziła dla swoich sieci bardziej rozbudowany protokół znakowy DDCMP, podczas gdy IBM zaproponował zorientowany bitowo SDLC. Protokół ten został w zasadniczym kształcie zaakceptowany przez ISO i jako standard o nazwie HDLC wprowadzony do wielu sieci komputerowych. Wybrane cechy wymienionych powyżej protokołów zestawione są w tabeli 3.1. Poza wymienionymi protokołami istnieje szereg innych proponowanych dla WŁD. Protokoły BSC, DDCMP, SDLC, HDLC i jego wersje (LAPB i LAPD) są jednakże najpopularniejsze. W dalszej części rozdziału dokonamy opisu wymienionych powyżej protokołów. Opis ten poprzedzimy analizą systemów z przepłytywaniem, biorąc pod uwagę fakt, że mechanizm przepłytywania jest wbudowany w większość popularnych protokołów WŁD dla sieci WAN.

Tabela 3.1. Porównanie wybranych protokołów WŁD

	BISYNC	DDCMP	SDLC	HDLC
Twórca	IBM	DEC	IBM	ISO
Dupleks	Nie	Tak	Tak	Tak
Półdupleks	Tak	Tak	Tak	Tak
Transmisja szeregową	Tak	Tak	Tak	Tak
Transmisja równoległa	Nie	Tak	Nie	Nie
Przeźroczystość	stuffing znakowy	liczenie znaków	stuffing bitowy	stuffing bitowy
Transmisja asynchroniczna	Nie	Tak	Nie	Nie
Transmisja synchroniczna	Tak	Tak	Tak	Tak
Transmisja punkt-punkt	Tak	Tak	Tak	Tak
Transmisja wielopunktowa	Tak	Tak	Tak	Tak
Adresacja stacji (połączenia wielopunktowe)	Opcjonalny nagłówek	Nagłówek	1 lub większa liczba bajtów	
Wykrywanie błędów	CRC-16/12 (VRC/LRC)	CRC-16 (Nagłówek + Dane)	CRC - CCITT	CRC - CCITT
Wykrywanie błędów w:	jedynie w tekście danych	nagłówku i danych oddzielnie	całej ramce	całej ramce
Zapobieganie utracie ramek	SAW	GBN	GBN	GBN lub SR

Tabela 3.1. Porównanie wybranych protokołów WŁD (c.d.)

	BISYNC	DDCMP	SDLC	HDLC
Rozmiar okna	1	255	7/127	7/127
Kod znakowy	ASCII EBCDIC	ASCII (jedynie znaki kontrolne)	dowolny	dowolny
Znaki sterujące (kontrolne)	wiele	DLE, ENQ, SYN, SOH	flaga	flaga
Formaty ramek	różne (liczne)	1 (3 typy)	1 (3 typy)	1 (3 typy)
Zarządzanie połączeniem	opcjonalny nagłówek	nagłówek	1 lub 2 bajty	1 lub 2 bajty
Ramkowanie	start 2 SYN koniec FTX/ETB	2 SYN liczba znaków	flaga flaga	flaga flaga
Sterowanie przepływem	znaki sterujące	brak (dane niszczone)	pole sterujące i mechanizm okienkowy	ramka RNR i mechanizm okienkowy

Przedmiotem naszego zainteresowania będą więc zarówno tzw. protokoły znakowe jak i znajdujące powszechnie zastosowanie we współczesnych systemach transmisji danych protokoły bitowe. Przykładami protokołów znakowych będą BISYNC oraz DDCMP. Z kolei w grupie protokołów bitowych rozważamy SDLC, HDLC, LAP, LAPB, LAPD. Pojęcie protokołu znakowego (bądź zorientowanego znakowo) oznacza, że w procesie nadawania/odbioru ramek interpretujemy znaczenie całych znaków, a w przypadkach koniecznych realizujemy stuffing znakowy. Specjalne znaki pełnią ważne funkcje umożliwiające zarówno synchronizację pracy stacji nadawczo/odbiorczych jak i separację kolejnych pól przesyłanych ramek informacyjnych, a w przypadku ramek sterujących znaki te w sposób jednoznaczny definiują znaczenie tych ramek. W protokołach zorientowanych bitowo rezygnujemy z rezerwacji pewnej grupy znaków do celów sterowania. Jedynym zarezerwowanym zwykle ciągiem bitów jest ciąg preambuły (wzorcowy ciąg synchronizacyjny), którego pojawiienie się w ciągu danych wymaga realizacji procedur stuffingu. Procedury bitowe są znacznie efektywniejsze od procedur znakowych. Tym niemniej realizacja procedur znakowych w oparciu o technikę VLSI jest zwykle prostsza. Organizacja pracy WŁD została przedstawiona w podrozdziale 2.1 Z kolei w podrozdziale 2.2 zostały też podane podstawowe zasady sterowania przepływem informacji pomiędzy obiektami WŁD; protokoły SAW, GBN i SR. W niniejszym rozdziale skoncentrujemy się na prezentacji wybranych protokołów warstwy łącza danych implementowanych w sieciach WAN.

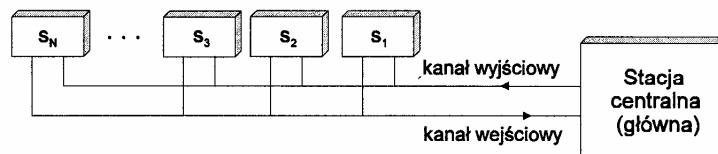
Wszystkie stosowane w praktyce protokoły WŁD pozwalają na realizację transmisji zarówno typu punkt-punkt jak też transmisji wielopunktowej (punkt do

### 3.1 Systemy z przepływaniem

wielopunktów). W tym drugim przypadku realizowane są procedury przepływania. Z uwagi na to, że przepływanie jest integralną częścią algorytmów WŁD w sieciach WAN, a także stanowi pierwotny rozproszony metod tokenowych, zagadnienu temu poświęcimy paragraf 3.1, poprzedzający prezentację wybranych protokołów znakowych i bitowych.

### 3.1 Systemy z przepływaniem

W przypadku gdy wspólne medium transmisyjne wykorzystywane jest przez większą liczbę stacji, konieczne staje się ustalenie zasad efektywnego dostępu do medium. Istnieją w zasadzie dwa sposoby rozwiązywania tego problemu. Pierwszy z nich wiąże się z przypadkowym (zdecentralizowanym) bądź rywalizacyjnym dostępem (por. ALOHA, S-ALOHA, CSMA, CSMA/CD), drugi natomiast określany jest mianem dostępu kontrolowanego. W tym przypadku dostęp może być sterowany bądź centralnie za pośrednictwem wydzielonej stacji bądź też w sposób rozproszony poprzez przekazywanie specjalnego znacznika (przepustki) - tokena (sposób ten jest stosowany, np. w standardowych rozwiązaniach sieci LAN).



Rys. 3.1. Przykładowa konfiguracja wielopunktowa ze sterowaniem centralnym

**Przepływanie** (ang. *polling*) jest pojęciem pierwotnym dla określenia drugiej klasy reguł dostępu. **Technika pollingu** była historycznie pierwszą, lecz ciągle powszechnie stosowaną metodą komunikowania się wielu stacji podległych z wybraną stacją centralną. Terminy łączności wielopunktowej lub połączeń wieloodczepowych (patrz rysunek 3.1) są zwykle używane dla określenia konfiguracji stacji stosujących metodę decentralizowanego przepływanego. Możliwość realizacji procesu przepływanego stacji jest integralną cechą wszystkich standardowych protokołów warstwy łącza danych projektowanych przede wszystkim z myślą o połączeniach typu punkt-punkt w sieciach rozległych (por. np. BSC, SDLC, HDLC, itd.). W przypadku stosowania pollingu, stacje są przepływanie indywidualnie w celu wyeliminowania rywalizacji w dostępie. Przykładami technik przepływanego są:

- metoda przepływania okrężnego (ang. *roll-call polling*) oraz
- metoda przepływania z przekazywaniem zapytania (ang. *hub polling*).

W pierwszej metodzie stacja główna (nadziedzona) przepływa stacje indywidualnie zgodnie z narzuconym lub przyjętym adaptacyjnie porządkiem. W drugiej

metodzie token (znacznik) jest cyklicznie przekazywany od stacji do stacji, a stacja główna nadzoruje jedynie ten proces.

### 3.1.1 Przepetywanie okrężne (indywidualne)

W tym typie strategii dostępu, *stacje są zapytywane kolejno przez stację główną, jedna po drugiej, czy mają one wiadomości do przesłania*. Stacja mająca informacje do przesłania dokonuje transmisji i powiadamia stację główną o zakończeniu tego procesu. Z kolei kontroler, tj. stacja centralna, przesyła zapytanie (kanałem wyjściowym) do stacji następnej na liście. Przepetywanie może być realizowane zarówno periodycznie ze stałym cyklem jak też adaptacyjnie, tj. z uwzględnieniem zmian w obciążeniu stacji. Może ono też uwzględniać priorytety w dostępie stacji do medium. Przepetywanie okrężne (ang. *roll-call polling*) stanowi jedną z opcji np. protokołów HDLC, DDCMP, BSC i SDLC.

### 3.1.2 Przepetywanie z przekazywaniem przepustki

*W przypadku realizacji przepetywania z przekazywaniem znacznika (tokena) prawo dostępu do medium przekazywane jest stacjom kolejno, przy czym proces ten, inicjowany przez stację główną, rozpoczyna się od stacji  $S_1$ , tj. najodleglejszej od centralnego kontrolera. Stacja  $S_1$  na zakończenie transmisji ramek dołącza do ostatniej z nich adres stacji  $S_{N-1}$ .* Ta z kolei po rozpoznaniu swojego adresu nadaje zgromadzone w buforach stacji ramki informacyjne, bądź, w przypadku ich braku generuje ramkę sterującą z dołączonym adresem stacji  $S_{N-2}$ . *Proces ten jest kontynuowany do chwili, gdy stacja  $S_1$  zakończy obsługę swoich ramek, dołączając do ostatniej z nich adres stacji głównej.* Po realizacji pełnego cyklu obsługi użytkowników sieci, centralny kontroler inicjuje zwykłe kolejną rundę przydziału dostępu do medium.

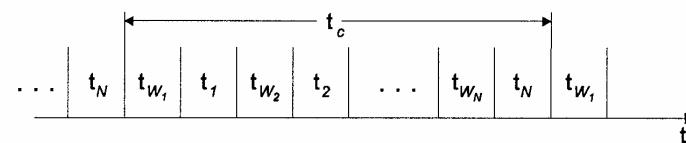
Należy zwrócić uwagę na fakt, że podobnie jak w systemie z przepetywaniem indywidualnym adresatem ramek przesyłanych przez stacje końcowe jest stacja centralna. W celu prawidłowego przebiegu procesu sterowania dostępem do medium użytkownicy muszą nie tylko słuchać transmisji, analizować adresy przesyłane kanałem wyjściowym, jak to ma miejsce w systemie z przepetywaniem indywidualnym (okrężnym), lecz także odbierać i analizować sygnały przesyłane kanałem wejściowym (patrz rysunek 3.1).

Pociąga to za sobą większą złożoność i wyższy koszt wyposażenia stacji, powodując jednocześnie, że stosowanie tego algorytmu w skoncentrowanych rozwiązańach sieciowych jest mniej powszechnie niż algorytm omawiany poprzednio, tj. z przepetywaniem indywidualnym. Należy jednak zwrócić uwagę na fakt, że przepetywanie z przekazywaniem tokena-zapytania zapewnia istotne skrócenie średniego czasu oczekiwania na dostęp do medium; szczególnie w sieciach w których odległości między stacjami końcowymi, a centralnym kontrolerem są znaczne. Koncepcja rozproszonego (zdecentralizowanego) sterowania przekazywaniem tokena realizowana jest w standardowych rozwiązańach sieci LAN (IEEE 802.4 i 802.5).

### 3.1.3 Uproszczona analiza jakości systemu z przepetywaniem indywidualnym

Jednym z podstawowych parametrów systemu z przepetywaniem jest opóźnienie  $D$  w obsłudze ramek informacyjnych napływających do buforów stacji, liczone jako czas upływający od chwili zgłoszenia się ramki do momentu zakończenia jej transmisji. Zakładając poissonowski strumień zgłoszeń do buforów wartość tego opóźnienia możemy przedstawić w postaci dwóch składników. Pierwszy z nich, odpowiadający czasowi transmisji ramek z danej stacji, może być wyrażony jako czas przebywania ramki w kolejce systemu M/G/1. Drugi natomiast jest w przybliżeniu połową cyklu przepetywania; czas ten intuicyjnie odpowiada okresowi oczekiwania stacji na rozpoczęcie obsługi. Przy małym obciążeniu stacji dominującą rolę odgrywać będzie składnik drugi. Z kolei przy wzroście intensywności zgłoszeń należy uwzględnić oba składniki, gdyż czas opóźnienia w obsłudze rośnie na skutek konieczności obsługi ramek, które napłynęły wcześniej (wyraża to czas oczekiwania na obsługę w systemie M/G/1). Czas trwania cyklu przepetywania  $t_c$  zależy od liczby ramek (zgłoszeń) czekających na transmisję. Na czas pojedynczego cyklu  $t_c$  składają się przy tym, zgodnie z ilustracją podaną na rysunku 3.2,

- czas przesyłania pozwoleń na transmisję ( $t_w$ ) oraz
- czasy trwania transmisji ramek ( $t_i$ ).



Rys. 3.2. Ilustracja cyklu w systemie z przepetywaniem

Pierwszy elementarny komponent czasowy,  $t_w$ , nazywany też czasem przepetywania (ang. *walk time*) zawiera czas wymagany na przesłanie ramki zapytania, synchronizację pracy oraz czasy propagacji w przekazywaniu zapytania. Czas trwania pojedynczego cyklu można opisać jako:

$$t_c = \sum_{i=1}^N t_{w_i} + \sum_{i=1}^N t_i$$

Długość cyklu jest losowa z uwagi na jej zależność od liczby zgłoszeń oczekujących na obsługę. Również czasy przepetywania można traktować jako realizacje pewnej zmiennej losowej. Dalej, przyjmiemy jednakże, że całkowity średni czas poświęcony na przepetywanie jest znany i wynosi  $T_w$ . Tym samym przedmiotem naszego zainteresowania będzie analityczna postać wyrażenia  $\sum_{i=1}^N t_i$ . Założymy przy tym:

- nieograniczone pojemności buforów stacji,
- średnią intensywność zgłoszeń (ramek) do bufora i-tej stacji równą  $\lambda_i$  ramek/s]
- średnią długość zgłoszeń (ramek) wyrażoną w jednostkach czasu równą  $m_i=F/c$  [s].

Przy powyższych założeniach średnia liczba ramek oczekujących na obsługę w zapytywanej i-tej stacji wynosi  $\lambda_i T_c$ ; gdzie  $T_c$  jest średnim czasem cyklu. Tym samym czas transmisji ramek jest równy

$$T_i = \lambda_i T_c m_i = \rho_i T_c$$

gdzie  $T_i$  jest średnio czasem obsługi (transmisji) w przypadku, gdy obciążenie i-tej stacji wynosi  $\rho_i = \lambda_i m_i$ .

Uwzględniając powyższe zależności mamy:

$$T_c = L / \left(1 - \sum_{i=1}^N \rho_i\right) = L / (1 - \rho)$$

gdzie

$$\rho = \sum_{i=1}^N \rho_i \text{ opisuje całkowite obciążenie wspólnego kanału.}$$

Wyrażenie na średnią długość cyklu  $T_c$  odgrywa kluczową rolę w określeniu średniego opóźnienia  $D$  w obsłudze ramek. Jak wspomniano wcześniej, dla małych wartości  $\rho$  opóźnienie  $D$  może być przybliżone zależnością

$$D \approx T_c / 2; \quad \rho \ll 1.$$

Przy wzroście  $\rho$  analiza  $D$  staje się bardzo złożona, z uwagi na powiązania statystyczne między kolejkami w buforach stacji.

Zakładając jednorodność systemu, tj. przyjmując  $\lambda_i = \lambda, m_i = m$  oraz geometryczny rozkład długości ramek otrzymujemy:

$$D = \frac{T_c}{2} \left(1 - \frac{\rho}{N}\right) + \frac{N\bar{m}^2}{2(1-\rho)} = \frac{L(1-\rho/N)}{2(1-\rho)} + \frac{N\lambda\bar{m}^2}{2(1-\rho)}$$

gdzie

$\bar{m}^2$  - jest drugim momentem długości ramki, a  $\rho = N\lambda m$ .

Z analizy powyższej zależności na czas opóźnienia  $D$  wynika, że system z przepisywaniem jako całość jest równoważny systemowi masowej obsługi typu M/G/1 z jedną wspólną kolejką zgłoszeń (ramek) obsługiwany zgodnie z FIFO (ang. First In-First Out). Jedyna różnica dotyczy dodatkowego czasu  $T_c/2$  związanego ze średnim czasem oczekiwania danej stacji na prawo dostępu do medium.

### 3.2 BISYNC (BSC) - Protokół ze znakami sterującymi

**Protokół BISYNC** (ang. *Binary Synchronous Communications* - BSC lub BISYNC) został zaproponowany i wdrożony w systemach komputerowych IBM; pierwotnie w systemach zdalnego przetwarzania wsadowego. *Jest on protokołem znakowym i zapewnia synchroniczny przekaz kodowanych binarnie ciągów danych.* Od chwili opracowania przez IBM nowego protokołu SDLC wykorzystanie BSC ulega stałemu ograniczeniu.

#### 3.2.1 Podstawowe zasady pracy protokołu

Podobnie do innych protokołów znakowych, BSC korzysta przy tworzeniu znaków sterująco-kontrolnych lub specjalnych znaków rozdzielających różne pola w przesyłanych ramkach z wybranych znaków popularnych kodów ASCII lub EBCDIC. Przykładowe kody znaków ASCII i EBCDIC i ich interpretacje podane są w tabeli 3.2.

Tabela 3.2. Kody znaków kontrolnych a) w 7-bitowym kodzie ASCII (ang. *American Standards Committee for Information Interchange*) zaakceptowanym przez CCITT (IA5 - International Alphabet Number 5) oraz ISO (ISO 645); b) w 8-bitowym kodzie EBCDIC (ang. *Extended Binary Coded Decimal Interchange Code*) firmy IBM  
a)

	4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
pozycje	3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1
bitów	2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1
	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
	7	6	5													
	0	0	0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF
	0	0	1	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	CR
	0	0	1												GS	RS
	0	0	1												US	

b)

	4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
pozycje	3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1
bitów	2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1
	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
	8	7	6	5												
	0	0	0	0	NUL	SOH	STX	ETX	PF	HT	LC	DEL			SMM	VT
	0	0	0	1	DLE	DC1	DC2	DC3	RES	NL	BS	IL	CAN	EM	CC	FF
	0	0	0	1											IGS	IRS
	0	0	1	0	DS	SOS	FS		BYP	LF	EOB	PRE			SM	IUS
	0	0	1	1				SYN	PN	RS	UC	EOT			DC4	NAK
	0	0	1	1											SUB	

DLE	- przejście do nowej ramki ( <i>Data Link Escape</i> )
SOH	- początek nagłówka ( <i>Start Of Header</i> ) - inicjuje początek nagłówka kolejnej wiadomości
STX	- początek danych ( <i>Start Of Text</i> ) - wskazuje początek tekstu wiadomości (ew. koniec nagłówka)
ETX	- koniec danych ( <i>End of Text</i> )
ETB	- koniec bloku danych ( <i>End of Transmission Block</i> )
EOT	- koniec transmisji ( <i>End Of Transmission</i> )
NAK	- negatywne powiadomienie ( <i>Negative Acknowledgment</i> )
ENQ	- żądanie połączenia ( <i>ENquiry</i> )
ACK0, ACK1	- powiadomienie pozytywne ( <i>positive ACKnowledgment</i> )
WACK	- wstrzymanie transmisji przed wysłaniem ACK ( <i>Wait before transmit positive ACK</i> )
RVI	- odwrotne przerwanie ( <i>ReVerse Interrupt</i> )
TTD	- chwilowe opóźnienie ( <i>Temporary Text Delay</i> )

**BISYNC jest protokołem znajdującym zastosowanie przy szeregowej, pół-dupleksowej**, tj. naprzemiennej transmisji danych. Może więc być stosowany do komunikacji punkt-punkt bądź punkt-wielopunkt. W przypadku komunikacji punkt-punkt połączenie obiektów WŁD może być dokonane z wykorzystaniem łączą komutowanego bądź dedykowanego. **Sterowanie przepływem ramek odbywa się zgodnie z algorytmem Stop-and-Wait (SAW).** W przypadku komunikacji wielopunktowej jedna ze stacji przejmuje rolę stacji głównej, sterującej wymianą informacji, podczas gdy pozostałe uczestniczące w wymianie stacje są podporządkowane. **Wielopunktowa wymiana informacji wymaga zwykle łączy dedykowanych (dzierżawionych), a transmisja realizowana jest zgodnie z zasadami przepływu indywidualnego.** Wyróżnia się przy tym dwa tryby pracy: tryb przepływu (ang. *polling mode*), gdy stacja główna zaprasza stacje podrzędne do przesyłania przygotowanych przez te stacje informacji oraz tzw. tryb selekcji (ang. *selection mode*), w którym stacja główna żąda potwierdzenia przez stację podporządkowaną jej gotowości do odbioru ramek informacyjnych, które mają być do niej przesłane przez stację główną.

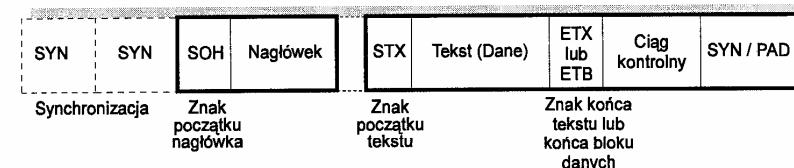
W przypadku połączeń punkt-punkt oprócz niezrównoważonego trybu pracy (ze sterowaniem połączeniem przez jedną ze stacji) dopuszcza się pracę stacji zgodnie z trybem zrównoważonym; oznacza to, że obie stacje mają identyczne prawa do inicjowania transmisji. W trybie tym mogą jednakże wystąpić kolizje przesyłanych ramek, wymagające rozwiązań zaistniałych konfliktów.

### 3.2.2 Format ramki

Przykładowy format ramki stosowany w BSC pokazany jest na rysunku 3.3. Znaki sterujące są wykorzystywane do określenia początków i końców poszczególnych fragmentów ramki. Pole danych może mieć w BSC zmienną długość. Może też być ono definiowane jako zawierające "przezroczyste" dane nie podle-

### 3.2 BISYNC (BSC) - Protokół ze znakami sterującymi

gajace żadnym przekształceniom w procesie transmisji. W takim przypadku pole danych zaczyna się znakami DLE STX, a kończy znakami DLE ETX (lub DLE ETB). Czas pomiędzy kolejnymi ramkami jest wypełniany przesyłanymi w sposób ciągły znacznikami PAD.



Rys. 3.3. Format ramki BSC

W protokole stosowane są następujące znaki sterujące:

DLE	- przejście do nowej ramki ( <i>Data Link Escape</i> )
SOH	- początek nagłówka ( <i>Start Of Header</i> ) - inicjuje początek nagłówka kolejnej wiadomości
STX	- początek danych ( <i>Start of Text</i> ) - wskazuje początek tekstu wiadomości (ew. koniec nagłówka)
ETX	- koniec danych ( <i>End of Text</i> )
ETB	- koniec bloku danych ( <i>End of Transmission Block</i> )
EOT	- koniec transmisji ( <i>End Of Transmission</i> )
NAK	- negatywne powiadomienie ( <i>Negative Acknowledgment</i> )
ENQ	- żądanie połączenia ( <i>ENquiry</i> )
ACK0, ACK1	- powiadomienie pozytywne ( <i>positive ACKnowledgment</i> )
WACK	- wstrzymanie transmisji przed wysłaniem ACK ( <i>Wait before transmit positive ACK</i> )
RVI	- odwrotne przerwanie ( <i>ReVerse Interrupt</i> )
TTD	- chwilowe opóźnienie ( <i>Temporary Text Delay</i> )

Kody znakowe używane przy transmisji mogą być zarówno typu ASCII, EBCDIC jak też sześciobitowe kodu TRANSCODE. Pewne elementy alfabetu są przy tym zarezerwowane jedynie dla znaków sterująco-kontrolnych, takich jak: SOH, STX, ETX, ITB, ETB, NAK, DLE oraz ENQ.

W protokole BSC używane są też dwuznakowe ciągi. Odnoszą się one do następujących znaków sterujących WACK, ACK0, ACK1, RVI i TTD. Dwie postacie powiadomień pozytywnych ACK, tj. ACK0 (do powiadamiania ramek nieparzystych) i ACK1 (do powiadamiania ramek parzystych) pozwalają za-

pewnić jednoznaczną interpretację ramek informacyjnych numerowanych binarnie (modulo 2). Powiadomienia ACK0 i ACK1 są kodowane znakami DLE0 i DLE1, w przypadku kodu ASCII, względnie DLE70H i DLE61H w przypadku alfabetu EBCDIC. Rozmiar i postać nagłówka są w protokole BSC opcjonalne. Gdy zawartość nagłówka definiowana jest przez użytkownika pole, to zaczyna się znakiem SOH i kończy STX.

Przepisywanie stacji podległych, ich adresacja, selekcja i zaproszenie do nadawania w połączeniach wielopunktowych są realizowane za pośrednictwem specjalnych ramek sterujących, a nie poprzez informacje zawarte w nagłówku ramki informacyjnej.

### 3.2.3 Wykrywanie błędów w transmisji

Ostatnim polem ramki informacyjnej BSC jest pole kontrolne tworzone przez bity nadmiarowe kodu parzystości wzdużnej bądź kodu cyklicznego. Kontrola błędów obejmuje głównie tekst ramki informacyjnej. Zabezpieczany fragment ramki rozpoczyna się więc po znaku STX - inicjującym pole danych, bądź po znaku SOH - inicjującym nagłówek, o ile jest on zawarty w ramce. Znaki zabezpieczenia kodowego następują po zakończeniu wiadomości lub bloku oznaczonego znakami ETX lub ETB. Wykorzystywany w protokole kod zabezpieczający transmisję przed błędami zależy przy tym od stosowanego w danym rozwiązaniu kodu znakowego. W przypadku kodu ASCII, każdy 7-bitowy znak ma dodatkowo jeden bit parzystości poprzecznej, a stosowany do zabezpieczania ramki ciąg kodowy jest pojedynczym 8-mio bitowym znakiem parzystości wzdużnej (LRC8). Kod EBCDIC wykorzystuje znaki 8-mio bitowe. W tym przypadku nie można realizować testów parzystości poprzecznej. Zatem jako zabezpieczenie kodowe ramki dodawane są w polu kontrolnym bity nadmiarowe kodu cyklicznego; są to dwa ósmiobitowe znaki CRC (CRC-16, tzn. generowane przez wielomian stopnia 16-tego). W stosowanym rzadziej kodzie TRANSCODE, będą to z kolei dwa znaki 6-cio bitowe (CRC-12).

W przypadku niezgodności testów kontrolnych CRC lub LRC w odebranej ramce, stacja odbiorcza przesyła powiadomienie negatywne NAK. Ramki informacyjne, w których spełnione są testy zgodności, powiadamiane są pozytywnie ramką kontrolną ACK0, dla ramek informacyjnych o numerach nieparzystych, bądź ramką ACK1, w przypadku ramek informacyjnych parzystych. Użycie różnych ramek typu ACK pozwala na identyfikację duplikatów oraz wykrywanie ramek brakujących.

W przypadku odbioru ramki NAK nadawca retransmituje cały blok, w którym wystąpił błąd. Kolejne ramki NAK stanowią informację o niesprawności łącza i powodują wstrzymanie transmisji.

### 3.2.4 Ramkowanie i synchronizacja transmisji

Przesyłane ramki mają w protokole BSC ściśle określona strukturę i są tworzone ze znaków wymienionych powyżej kodów. Protokół BSC dopuszcza jednakże

obok normalnego trybu transmisji tzw. przeźroczysty tryb transmisji, pozwalający na tworzenie tekstu ramki z wykorzystaniem dowolnego kodu.

Przeźroczysty tryb pracy stacji wymuszany jest przez rozpoczęcie pola danych znakami DLE STX. Jedynym znakiem sterującym rozpoznawanym (i interpretowanym) przez proces odbiorczy warstwy WLD jest wówczas DLE (początek nowego bloku danych). Wszystkie znaki sterujące przesyłane w tym trybie muszą być również poprzedzane przez DLE, w celu ich realizacji. Jednoznaczna interpretacja znaków w polu danych ramki wymaga dodawania znaku DLE każdorazowo, gdy przesyłany ciąg bitów odpowiada znakowi DLE (stuffing znakowy).

Zasady synchronizacji w protokole BSC wymagają, by transmisja każdej ramki informacyjnej bądź kontrolnej poprzedzona była znakami SYN. Znak SYN jest przy tym ciągiem bitów jednoznacznie rozpoznawanym przez styrk sprzętowy stacji i pozwalającym na odtworzenie synchronizacji znakowej. Znaki SYN mogą być dodatkowo poprzedzane sekwencją bitów 101010... w celu zapewnienia zarówno synchronizacji bitowej jak też zagwarantowania stacji odbiorczej wystarczającego przedziału czasu na przygotowanie się do rozpoczęcia realizacji procedur odbiorczych. Przy normalnym trybie pracy, ramki są poprzedzane dwoma znakami SYN, podczas gdy przy trybie przeźroczystym - znakami DLE SYN.

Praca wielopunktowa stacji inicjowana jest w trybie przepisywania (zaproszenia do nadawania) przesłaniem ciągu sterującego o postaci PAD SYN EOT SYN PAD (adres stacji podrzędnej zaproszonej do nadawania) ENQ PAD. Ciąg ten rozpoznawany przez stacje podrzędne, jest przez nie interpretowany jako zaproszenie do nadawania ramki do stacji centralnej. Informacja o adresie stacji zaproszonej do nadawania lub wskazanej jako adresat ramki ze stacji głównej (w trybie selekcji) składa się z od 1 do 7 znaków. Znak PAD rozpoczynający ramkę sterującą sygnalizuje zmianę kierunku transmisji, w kolejnej fazie przekazu informacji. W przypadku trybu selekcji wybór stacji o wskazanym w ramce adresie związany jest z przesłaniem ciągu SYN EOT PAD SYN (adres stacji podrzędnej wskazanej jako adresat) ENQ PAD.

Protokół BSC definiuje następujące odpowiedzi ze strony stacji podrzędnej zaproszonej do transmisji:

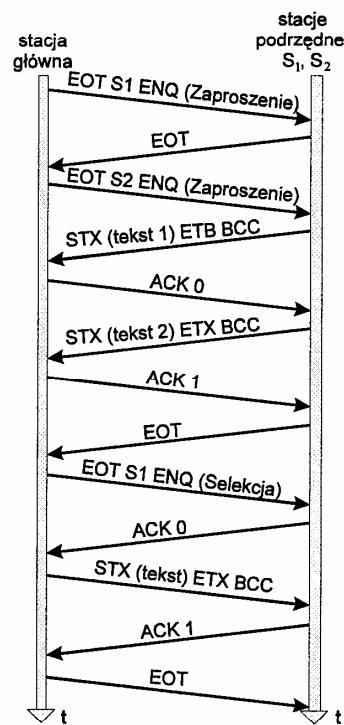
- ramka z nagłówkiem (SYN SOH ...)
- dane bez nagłówka (SYN STX dane ...)
- dane w trybie przeźroczystym (SYN DLE STX przeźroczyste dane ...)
- odpowiedź negatywna, w przypadku braku danych do przesłania (SYN EOT)
- informacja o czasowym opóźnieniu w przesłaniu danych; gdy stacja nie może rozpocząć pracy w ciągu 2 sekund (SYN STX ENQ).

W przypadku stacji wskazanej jako odbiorca ramki ze stacji głównej, możliwe są następujące rodzaje odpowiedzi:

- a) potwierdzenie gotowości do odbioru (SYN ACK SYN),
- b) informacja o braku gotowości do odbioru (SYN NAK),
- c) informacja o czasowym braku gotowości do odbioru (SYN WACK).

Wszystkie podane powyżej rodzaje ramek odpowiedzi zaczynają się i kończą znakami PAD.

### 3.2.5 Przykładowe procedury sterowania transmisją ramek

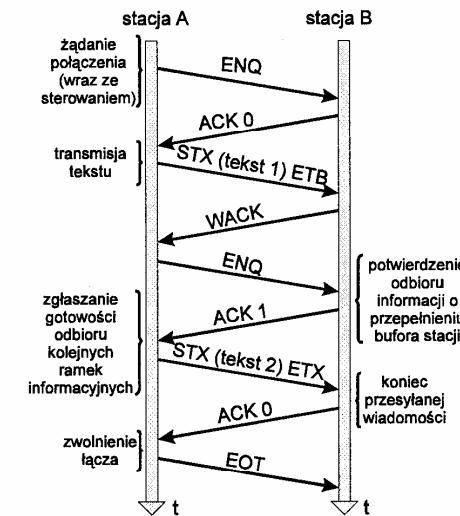


Rys. 3.4. Przykładowa wymiana informacji pomiędzy stacją główną, a stacjami podrzędnymi  $S_1$  i  $S_2$ . Na ilustracji pominięto znaki SYN i PAD.  
BCC - oznacza pole zabezpieczenia kodowego (ang. Block Check Code)

Zaproponujemy obecnie wybrane procedury sterowania połączeniem typu punkt-punkt oraz połączeniem wielopunktowym. Na wstępnie rozważymy przypadek wielopunktowej wymiany informacji. Przykład takiej wymiany pomiędzy stacją główną i dwiema stacjami podrzędnymi pokazany jest na rysunku 3.4. Na ilustracji pominięto znaki PAD oraz znaki synchronizacji. W podanym przykładzie stacje podrzędne  $S_1$  i  $S_2$  są kolejno przepływanie przez stację główną,

W przypadku braku ramek informacyjnych do transmisji stacje podrzędne odpowiadają ramkami typu EOT (PAD SYN EOT PAD). Z kolei, gdy stacje posiadają wiadomość do przesłania, wówczas reagują na zaproszenie przesyłając kolejne bloki tekstu (PAD SYN SOH (nagłówek) STX (tekst) ETB BCC PAD). BCC (ang. Block Check Code) stanowi pole zabezpieczeń kodowych. Poprawny odbiór ramek informacyjnych jest powiadamiany zarówno przez stacje podrzędne jak i stację główną ramkami ACK0 i ACK1 (PAD SYN ACKi PAD). W przypadku, gdy stacja główna ma do przesłania informacje do jednej ze stacji podrzędnych, wówczas przechodzi ona do trybu pracy z selekcją stacji podrzędnej, wskazując jej adres w ramce EOT (adres  $S(i)$ ) ENQ.

W przypadku połączeń typu punkt-punkt procedura transmisji jest prostsza, gdyż zarówno nadawca jak i odbiorca wiadomości są znani a priori. Tym samym komendy - ramki zapytania i selekcji mogą być przesyłane bez adresów. W tym typie połączenia możliwe są dwie wersje komunikacji między stacjami, a mianowicie tryb niezrównoważony z zachowaniem wyżej omówionych zasad oraz tryb zrównoważony dopuszczający rywalizację stacji o prawo do nadawania.



Rys. 3.5. Ilustracja wymiany informacji w trybie zrównoważonym

W trybie zrównoważonym (tryb rywalizacji) obie stacje mogą inicjować wymianę wiadomości; przebieg tej wymiany może mieć postać pokazaną na rysunku 3.5. Stacja chcącą nadać blok informacyjny przesyła komendę - ramkę ENQ żądania przejęcia sterowania łączem. Jeżeli partner wymiany akceptuje to żądanie, to odpowiada ramką powiadomienia pozytywnego ACKi. Otrzymanie tego powiadomienia oznacza przejęcie sterowania łączem (podobnie jak w trybie

niezrównoważonym) do chwili rezygnacji z tego prawa poprzez przesłanie ramki typu EOT. Do tego momentu stacja sterująca może przesyłać serie bloków. W przypadku wystąpienia w stacji odbiorczej stanu przepełnienia jej buforów, stacja ta przesyła ramkę WACK oznaczającą jej chwilową niezdolność do akceptacji kolejnych bloków danych. Stacja nadająca wstrzymuje wtedy transmisję ramek informacyjnych przesyłając jednakże periodycznie komendy ENQ - do chwili odbioru powiadomienia pozytywnego. Zwróćmy uwagę na fakt, że wprowadzenie komendy WACK pozwala na uelastycznenie procedury sterowania przepływem informacji.

W trybie zrównoważonym może dojść do konfliktu stacji, tj. sytuacji, gdy obie stacje prawie równocześnie prześlą żądanie przejęcia sterowania pracą łączą. Stacje będą nie otrzymały wtedy żadnego potwierdzenia, bądź też odbiorą powiadomienia negatywne NAK. Powtarzają one wtedy transmisje ramek ENQ, przy czym *czasy randomizacji retransmisji* sa w obu stacjach różne.

W przypadku transmisji punkt-punkt stacja może zażądać zmiany prawa dostępu. W tym celu przesyła ona ramkę przerwania RVI (ang. *Reverse Interrupt*), zawierającą powiadomienie ramek odebranych przez tę stację i żądanie przejęcia kontroli nad łączem.

Inną, często stosowaną komendą sterującą jest ramka TTD (ang. *Temporary Text Delay*) pozwalającą na czasowe opóźnienie transmisji tekstu. Tego typu ramka - komenda przesyłana jest przez stację nadawczą, pragnącą zachować kontrolę nad łączem, gdy nie ma ona w danej chwili żadnej ramki informacyjnej gotowej do wysłania. Ramka TTD może też być wykorzystana do czasowego zawieszenia transmisji ramek informacyjnych, przed zakończeniem przesyłania całej wiadomości. Sytuacja taka może być np. związana z obserwowanym czasowo pogorszeniem się jakości transmisji.

### 3.3 Protokół znakowy DDCMP z liczeniem znaków

**Protokół DDCMP** (ang. *Digital Data Communications Message Protocol*) został opracowany przez firmę DEC (ang. *Digital Equipment Corporation*) z przeznaczeniem dla szerokiego zestawu sieci komputerowych (sieci synchroniczne i asynchroniczne, z kanałami dedykowanymi lub komutowanymi, pracującymi w trybie półduplexowym bądź duplexowym, z połączeniami typu punkt-punkt względnie punkt-wielopunkt). DDCMP może też współpracować z interfejsami przystosowanymi do transmisji szeregowej bądź równoległej (połączenia między procesorami lokalnymi).

### 3.3.1 Podstawowe zasady pracy protokołu

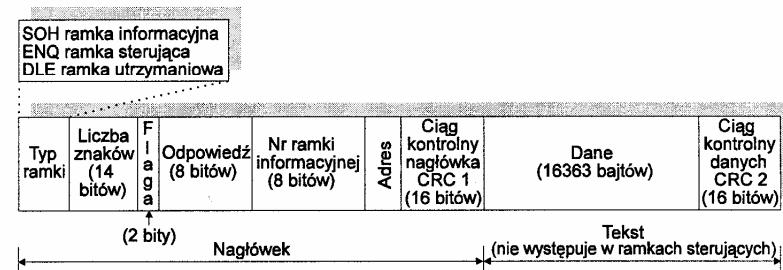
Protokół DDCMP, wprowadzony na rynek w 1975 r., był pierwotnie jedynym standardem DEC-owskim. Obecnie wraz z protokołem LAPB, z opracowanego przez CCITT standardu X.25, stanowi on jedna z opcji stosowanych w sieciach

DEC. W porównaniu z prezentowanym poprzednio protokołem BSC, protokół DDCMP charakteryzuje się znacznie większą uniwersalnością i elastycznością pracy.

Aby wyeliminować skomplikowane procedury, wymagane dla zapewnienia jednoznacznej i zrozumiałej interpretacji danych w BSC, firma DEC zaproponowała protokół, w którym proces ramkowania bloków danych realizowany jest poprzez liczenie bajtów. Zapewnia to przeźroczeńność danych (jednoznaczność ich interpretacji) bez używania specjalnych znaków sterujących. Taka metoda „ramkowania” danych ma jednakże pewne mankamenty.

### 3.3.2 Format ramki

Format ramki informacyjnej pokazany jest na rysunku 3.6. Ramka obejmuje nagłówek i blok danych. Nagłówek zawiera podstawowe informacje sterujące, w tym numer wiadomości i liczbę znaków bloku danych. Nagłówek posiada też własne 16-bitowe pole CRC, poprzedzające blok danych. Blok danych może zawierać do 16363 8-mio bitowych znaków. Blok ten zabezpieczony jest 16-bitowym ciągiem CRC. Ramki sterujące składają się wyłącznie z nagłówka (nie zawierają bloku danych i zabezpieczającego ten blok ciągu CRC).



Rys. 3.6. Format ramki DDCMI

W protokole DDCMP w celu dokonania rozróżnienia pomiędzy typami (klasami) ramek:

- informacyjnych (zawierających dane)
  - sterujących, i
  - kontrolnych (utrzymywanych)

używane sa wybrane znaki sterujace kodu ASCII. I tak stosujemy:

SOH - dla oznaczenia ramki informacyjnej,  
ENQ - dla oznaczenia ramki sterującej oraz  
DLE - dla ramki kontrolnej (utrzymywanej).

Początek ramki, z informacją o jej typie, jest zawsze poprzedzany znakami SYN zapewniającymi synchronizację znakową. Z kolei po polu typu ramki występuje

14-bitowe pole liczby znaków. W przypadku ramek informacyjnych i utrzymywanych pole to podaje liczbę znaków informacyjnych występujących po nagłówku. W ramkach sterujących 8 pierwszych bitów tego pola określa dokładnie typ tej ramki, podczas gdy pozostałe 6 bitów są zapełniane zerami, z wyjątkiem powiadomienia negatywnego NAK. - Wówczas 6 bitów identyfikuje przyczynę negatywnego powiadomienia. Dwubitowe pole flagi służy do przekazania np. informacji, że dana ramka jest ostatnią w przesyłanym ciągu i że stacja odbiorcza, w konfiguracji półdupleksowej lub wielopunktowej, może rozpoczęć swoją transmisję. Kolejne, ośmiobitowe pole odpowiedzi zawiera każdorazowo numer ostatniej poprawnie odebranej ramki. - Pole to odnosi się do ramek informacyjnych i sterujących typu ACK. Pole następne zawiera 8-bitowy numer ramki informacyjnej. W ramkach sterujących typu REP (ang. *repeat*) pole numeru ramki pozwala na przesłanie zapytania, czy wszystkie ramki o numerach do wskazanego w polu włącznie zostały odebrane poprawnie. 8-bitowy adres zawarty w kolejnym polu ramki wykorzystywany jest przy pracy wielopunktowej do wskazania stacji podlegającej jako adresata ramki bądź kolejnego nadawcy ramek. W połączeniach typu punkt-punkt pole adresu jest wypełniane bitami 1.

### 3.3.3 Wykrywanie błędów

Protokół DDCMP stosuje bardziej złożone i wyrafinowane algorytmy wykrywania i usuwania błędów niż omawiany poprzednio protokół BSC.

W przypadku wykrycia błędów poprzez kontrolę CRC specjalna ramka sterująca NAK przesyłana jest do stacji źródłowej. W przypadku ramek poprawnie transmitowanych nie wszystkie one są powiadamiane pozytywnie, gdyż numer w polu odpowiedzi ramki informacyjnej bądź sterującej ACK pozwala na potwierdzanie grupowe ramek. W przypadku pracy w trybie dupleksowym ramki NAK są dodawane do strumienia przesyłanych ramek informacyjnych; przez co nie ma potrzeby na wstrzymywanie transmisji jak w przypadku algorytmu Stop-and-Wait.

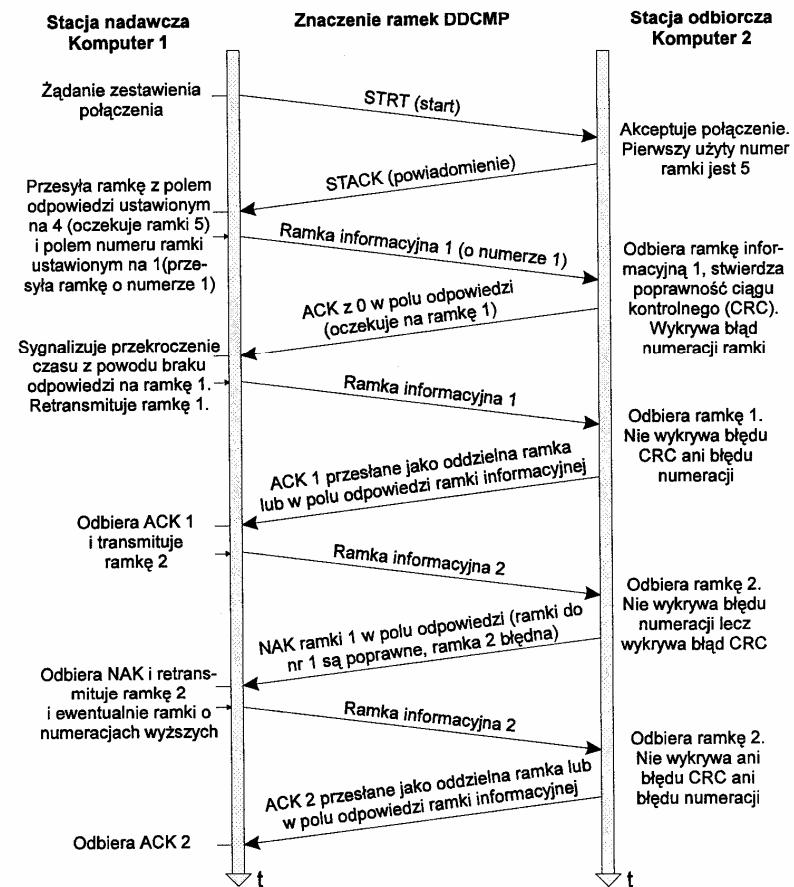
W protokole DDCMP realizowany jest algorytm retransmisji Go-Back-N; dopuszcza się przy tym transmisję do  $N=255$  niepotwierdzonych ramek informacyjnych. Pozwala to na uzyskanie wysokiej efektywności pracy protokołu w przypadku jego wykorzystania na łączach wnoszących duże opóźnienia propagacyjne (np. łączą satelitarne).

W przypadku pracy protokołu w konfiguracji wielopunktowej dopuszcza się jednakże przesyłanie jedynie do pięciu ramek, zarówno przez stację główną (nadrzędną) jak i stacje podrzędne.

Po odbiorze ramki o niewłaściwym numerze żadna odpowiedź nie jest przez stację generowana. Informacja o tym fakcie będzie przez stację nadawczą wykrywana poprzez kontrolę pola odpowiedzi w odbieranych ramkach informacyjnych.

W przypadku upływu time-out-u stacja nadawcza przesyła ramkę REP zawierającą numer najwcześniej niepotwierzonej ramki. Gdy stacja odbiorcza odebrała poprawnie wszystkie wskazane ramki, wówczas przesyła ramkę ACK. W przeciwnym przypadku generuje ramkę NAK zawierającą numer ostatniej prawidłowo odebranej ramki, a stacja nadawcza retransmituje wówczas wszystkie niepotwierdzone ramki.

Przykład jednokierunkowej i półdupleksowej wymiany informacji pokazany jest na rysunku 3.7.



Rys. 3.7. Ilustracja jednokierunkowej i półdupleksowej wymiany informacji w protokole DDCMP

W przypadku pracy dupleksowej powiadomienia ACK są przesyłane w polu odpowiedzi kolejnej ramki informacyjnej.

### 3.3.4 Synchronizacja i testowanie pracy stacji

Synchronizacja znakowa pracy stacji realizowana jest poprzez poprzedzenie każdej ramki dwoma znakami SYN. Znaki te nie są jednakże potrzebne w przypadku ciągłej pracy stacji. Synchronizacja znakowa nie jest też stosowana przy asynchronicznej transmisji szeregowej lub równoległawej. Znaki SYN nie mogą być ponadto stosowane wewnątrz ramki (w szczególności w polu danych), gdyż spowoduje to każdorazowo błąd w transmisji. Ramki utrzymaniowe (kontrolne) pozwalają na przesyłanie i realizację programów testujących. Ramki te rozpoczynają się znakami DLE. Pole danych w tych ramkach zawiera stosowny program.

## 3.4 Protokół bitowy SDLC

*Protokół SDLC* (ang. *Synchronous Data Link Control*) został zaprojektowany przez IBM jako część architektury SNA. *Był on pierwszym popularnym protokołem bitowym, a jednocześnie pierwowzorem protokołu HDLC. Protokoły zorientowane bitowo wykorzystują zwykle jeden standardowy typ ramki uwzględniający szereg parametrów kontrolno-sterujących oraz pole informacyjne (danych) zabezpieczone bitami kontrolnymi.* Podstawową zaletą tej klasy protokołów jest fakt, że oprogramowanie warstwy WŁD nie musi interpretować różnych znaków kontrolnych lub ich sekwencji. Nie dokonuje też ono zliczania tych znaków.

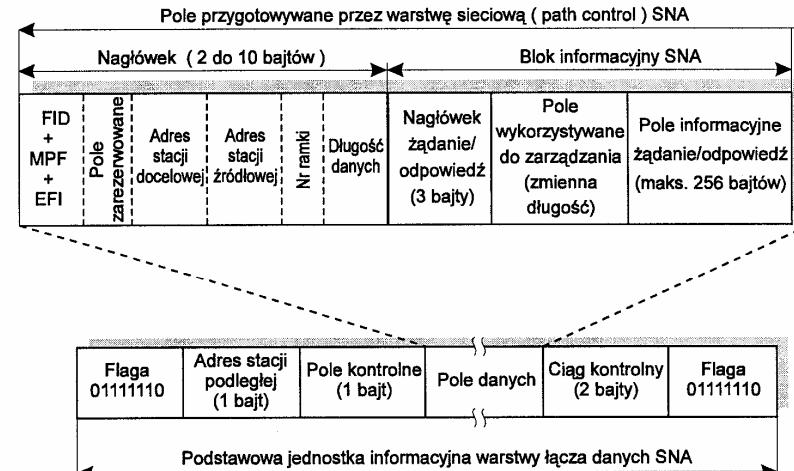
### 3.4.1 Podstawowe zasady pracy

SDLC jest dostosowany do pracy w trybie pełno- lub półduplexowym z wykorzystaniem łączni dedykowanych lub komutowanych z synchroniczną transmisją szeregową. Możliwa jest też praca w systemie o konfiguracji punkt-punkt lub punkt-wielopunkt. W trybie niezrównoważonym mającym miejsce w sieci z konfiguracją wielopunktową jedna ze stacji jest stacją główną (nadrzędną), pozostałe zaś są podległe. Tryb zrównoważony pracy, definiowany np. w protokole HDLC, nie jest w SDLC realizowany. Dopuszcza się jednakże, by w konfiguracji wielopunktowej stacje podległe inicjowały transmisję ramek.

Przy dupleksowym trybie pracy stacji SDLC jest protokołem bardzo efektywnym, mając znacznie krótszą część organizacyjno-sterującą ramki niż protokoły BSC lub DDCMP.

### 3.4.2 Format ramki

Standardowy format ramki protokołu SDLC wraz z definicjami poszczególnych pól pokazany jest na rysunku 3.8.



Rys. 3.8. Format ramki SDLC

W porównaniu z omawianymi wcześniej protokołami znakowymi, jedynym znakiem specjalnym jest flaga ramki, będąca ciągiem bitów o postaci 0111110, poczynającą i kończącą ramkę SDLC. Jednakże, gdy kolejne ramki przesyłane są bezpośrednio jedna po drugiej, wymagana jest tylko jedna flaga.

Aby zabezpieczyć ciągi bitów pola danych przed ich błędnią interpretacją jako flagi, po każdym 5-ciu jedynkach nadajnik stacji wprowadza dodatkowe zero, usuwane następnie po stronie odbiorczej. Stosowany w protokole stuffing bitowy nie zwiększa sum kontrolnych, gdyż dodawane (i usuwane zera) nie są objęte testami kontrolnymi (stuffing realizowany jest przez warstwę fizyczną WF).

Długość pola danych może być w SDLC dowolna, zmieniająca się od zera do pewnej górnej granicy określonej na podstawie częstości błędów w łączu. Nie ma przy tym jakichkolwiek ograniczeń ani na format danych ani na ich zawartość. W związku z tym dowolny kod informacyjny może być stosowany przy tworzeniu pola danych ramki.

Pole danych jest poprzedzane 8-mio bitowym adresem i 8-mio bitowym polem kontrolno-sterującym. Oba pola mogą być przy tym wydłużone; pole sterujące może być wydłużone do 16-stu bitów. Adres wskazuje numer stacji podległej (przy współpracy wielopunktowej), do której przesyłana jest (przez stację nadrzędną) dana komenda (ramka).

Wyróżnia się przy tym trzy typy ramek:

- 1) ramki przekazu danych (informacyjne),
- 2) ramki zarządzające,
- 3) ramki nienumerowane.

Ramki przekazu danych wykorzystywane są, zgodnie z ich nazwą, do przesyłania danych; są one numerowane. Ramki zarządzające są z kolei używane do inicjowania przekazu danych i sterowania jego przebiegiem. Ostatni typ ramek stosowany jest do ustalenia trybu pracy stacji oraz zapewnienia gotowości ich funkcjonowania.

Dwa pierwsze bity pola sterującego definiują typ ramki:

- 00 - ramki przekazu danych (ang. *information frames*)
- 10 - ramki zarządzające (ang. *supervisory frames*)
- 11 - ramki nienumerowane (ang. *unnumbered frames*)

Bit P/F pytanie/konczenie transmisji (ang. *poll/final*) pola sterującego, używany jest we wszystkich typach ramek. Oznacza on np. że ramka przesyłana ze stacji nadzędnej do podległej winna być traktowana jako zaproszenie do przesyłania danych, wówczas P/F=1. W przypadku odpowiedzi stacji podległej na zaproszenie stacji nadzędnej, P/F=0 dla początkowych ramek odpowiedzi oraz P/F=1 dla ostatniej ramki odpowiedzi.

### 3.4.3 Wykrywanie błędów i odtwarzanie ramek

Do zabezpieczania ramek przed błędami stosowany jest standardowy kod cykliczny (standard CCITT), generowany przez wielomian 16-stego stopnia (CRC-16). Zabezpieczenie to nie obejmuje samego CRC i flag.

Wszystkie ramki informacyjne (ramki przekazu danych) zawierają kolejne trzy-bitowe numery N(s) (zapisane w polu sterującym), a stacja odbiorcza przechowuje numer ostatniej bezbłędnie odebranej ramki. Na tej podstawie modyfikuje ona numer N(r) odpowiadający kolejnemu oczekiwaniu numerowi N(s) ramki. (por. zasady pracy algorytmów okienkowych).

Numer N(r) ramki oczekiwanej przez stację jest również przesyłany w polu sterującym z wykorzystaniem 3-ch bitów.

Ramki zarządzające stosowane w SDLC pozwalają na przekazywanie 3-ch dwubitowych informacji sterujących:

- RR - gotowość odbioru (ang. *receive ready*)
- RNR - brakgotowości odbioru (ang. *receive not ready*)
- REJ - odrzucenie (ang. *reject*)

RR oznacza, że wszystkie ramki o numerach do N(r)-1 zostały odebrane bezbłędnie, a stacja odbiorcza jest gotowa do przyjęcia następnych. RNR podobnie jak RR potwierdza poprawny odbiór ramek o numerach do N(r)-1 włącznie, lecz z uwagi na np. zajętość buforów odbiorczych stacja nie jest w stanie przyjąć kolejnych ramek. Z kolei REJ jest żądaniem transmisji lub retransmisji ramek o numerze N(r) i następnych. Ramki zarządzające RR i RNR spełniają funkcje ramek ACK z protokołów znakowych. Stosowana w SDLC procedura Go-Back-N dopuszcza jednakże transmisję maksymalnie 7 niepotwierdzonych ramek.

Okienko nadawcze jest bowiem w tym protokole 7-mio ramkowe. Wyjątek dotyczy stacji współpracujących po łączach satelitarnych, gdy okienko zostaje rozszerzone do 127 ramek. Ramka REJ pełni w SDLC funkcję NAK. Retransmisje ramek niepotwierdzonych realizowane są po upływie time-out-u.

Połączenie między stacjami może być zakończone procedurą przerwania. Stacja nadająca wysyła wówczas ciąg ośmiu jedynek, po których przesyłana jest flaga lub przynajmniej 7 dodatkowych jedynek. Po ich transmisji łącze jest wolne.

## 3.5 Protokół bitowy HDLC

Protokół HDLC (ang. *High level Data Link Control*) jest standardowym protokołem ISO. Opcje tego protokołu zostały też zaakceptowane przez CCITT w warstwie 2 standardu X.25, jako protokoły LAP (ang. *Link Access Procedure*) bądź LAP-B (ang. *Link Access Procedure-Balanced*).

### 3.5.1 Podstawowe informacje

Opracowany przez ISO **protokół HDLC jest, podobnie jak IBM-owski SDLC, protokołem bitowym**. Posiada on standardowy typ ramki z nieograniczonym polem danych, możliwością stosowania dowolnych kodów znakowych i kilkoma zarezerwowanymi dla celów sterujących sekwencjami bitów. Zapewnia to uproszczenie projektowania oprogramowania protokołu. Znaczne analogie do ISO-wskiej wersji HDLC można odnaleźć w protokołach:

- HDLC opracowanym przez ECMA,
- ADCCP (prawie identycznym jak HDLC) zaproponowanym przez ANSI, wymienianych wcześniej protokołach,
- LAP oraz LAP-B opracowanych przez CCITT,

jak też we wspomnianym

- IBM-owskim protokole SDLC (który posiada dodatkowe w stosunku do HDLC typy ramek z komendami i odpowiedziami).

**HDLC został zaprojektowany do współpracy z łączami synchronicznymi zarówno dupleksowymi jak i półdupleksowymi.**

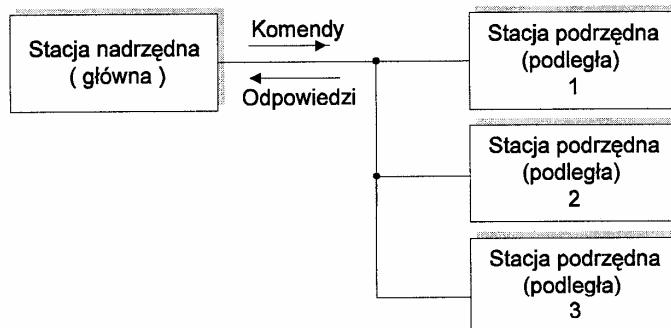
### 3.5.2 Konfiguracje logiczne HDLC

Protokół HDLC może pracować w jednej z trzech konfiguracji kanału logicznego:

- 1) niezrównoważonej,
- 2) zrównoważonej,
- 3) symetrycznej.

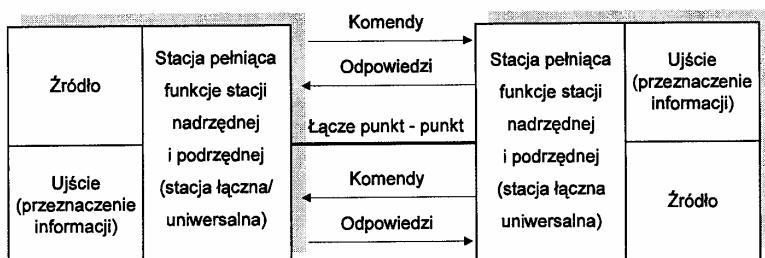
Zgodnie z HDLC stacja główna (nadzędna) transmituje ramki z komendami sterującymi i otrzymuje ramki odpowiedzi od stacji wtórznych (podzadnych), lub

podległych) w połączeniu punkt-punkt i w połączeniu wielopunktowym. W niezrównoważonej konfiguracji logicznej, która może być typu zarówno punkt-punkt jak i wielopunkt, występuje jedna stacja główna i jedna lub więcej podległych; zgodnie z ilustracją z rysunku 3.9. Możliwe są przy tym dwa tryby pracy: Normalny Tryb Odpowiedzi (ang. NRM - *Normal Response Mode*), w którym stacja główna przepytuje stacje podrzędne oraz Asynchroniczny Tryb Odpowiedzi (ang. ARM - *Asynchronous Response Mode*), w którym stacje nadzędne mogą transmitować w relacji stacja podrzędna-stacja główna nawet jednocześnie. Konfiguracja logiczna połączenia jest niezrównoważona, gdyż stacja główna steruje dostępem stacji podległych do kanału.



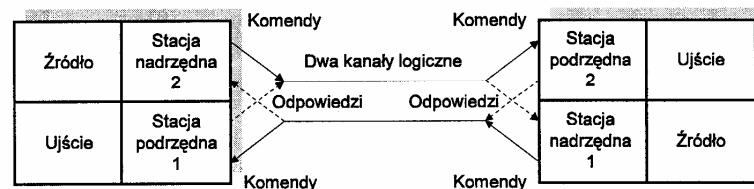
Rys. 3.9. Niezrównoważona konfiguracja logiczna HDLC

Konfiguracja zrównoważona pokazana na rysunku 3.10 odnosi się do współpracy dwóch stacji, z których każda ma te same prawa w przekazie danych i sterowaniu połączeniem typu punkt-punkt. Stacje mają więc cechy zarówno stacji głównej jak i podrzędnej; mówiąc wówczas możemy o stacji "łącznej" lub uniwersalnej. Z konfiguracją zrównoważoną wiąże się Asynchroniczny Zrównoważony Tryb Pracy (ang. ABM - *Asynchronous Balanced Mode*) stosowany w protokole LAP-B w X.25.



Rys. 3.10. Zrównoważona konfiguracja logiczna HDLC

Dwie niezrównoważone konfiguracje logiczne wykorzystywane w połączeniu punkt-punkt tworzą konfigurację symetryczną, zwielokrotnioną fizycznym łączem danych, zgodnie z ilustracją z rysunku 3.11. Dwa kanały logiczne łączą wówczas stacje główne i podrzędne, przy czym stacje główne (w każdej z dwóch konfiguracji niezrównoważonych) są odpowiedzialne za wybór trybu pracy. Konfiguracja ta stosowana jest w protokole LAP X.25.



Rys. 3.11. Ilustracja dwóch niezrównoważonych konfiguracji logicznych wykorzystywanych w połączeniu punkt-punkt

### 3.5.3 Stany logiczne i tryby pracy

Połączenie między stacjami wykorzystującymi HDLC może znajdować się w jednym z trzech stanów logicznych:

- stanie przekazu informacji (ang. ITS - *Information Transfer State*)
- stanie inicjowania pracy (ang. IS - *Initialization State*)
- stanie rozłączenia logicznego (ang. LDS - *Logically Disconnected State*).

W stanie ITS, stacja podrzędna lub uniwersalna może nadawać lub odbierać ramki informacyjne. Stacja osiąga ten stan, gdy zrealizowane zostaje połączenie logiczne zgodnie z NRM, ARM lub ABM.

W stanie inicjowania połączenia IS realizowane są procedury sterowane przez wyższe warstwy oprogramowania komunikacyjnego. Praca stacji podrzędnej lub uniwersalnej jest inicjowana przez odbiór zestawu parametrów ze stacji odległej.

Z kolei stan rozłączenia logicznego LDS powstrzymuje stację podrzędną lub uniwersalną przed transmisją lub odbiorem danych. Stan ten związany jest z realizacją procedur Asynchronicznego Trybu Rozłączenia (ang. ADM - *Asynchronous Disconnected Mode*) lub Normalnego Trybu Rozłączenia (ang. NDM - *Normal Disconnected Mode*).

W protokole HDLC wyróżniamy 6 trybów pracy, definiujących zasady przekazu informacji (3 tryby), rozłączenia (2 tryby) oraz inicjowania pracy stacji. Tryby przekazu danych to:

- **Normalny Tryb Odpowiedzi (NRM)** - Tryb ten stosowany jest w połączeniach typu punkt-punkt lub hierarchicznych połączeniach wielopunktowych (tj. o niezrównoważonej konfiguracji logicznej). Ustala on

podział stacji na główną (nadrzędną) i podległe. Stacja główna jest odpowiedzialna za nawiązanie połączenia i nadzorowanie jego przebiegu; łącznie z wykrywaniem błędów i niesprawności. Stacje podrzędne mogą jedynie odpowiadać na komendy przesyłane przez stację główną i przesyłać ramki informacyjne po otrzymaniu zaproszenia (zapytania). Wyposażenie stacji podległej może więc być dużo prostsze niż stacji głównej.

- **Asynchroniczny Tryb Odpowiedzi (ARM)** - Tryb ten stosowany jest, podobnie jak NRM, w połączeniach punkt-punkt lub wielopunktowych. W trybie tym wyróżniamy również stację główną i podległe. Zadaniem tej pierwszej jest nawiązanie połączenia oraz czuwanie nad poprawnością jego realizacji (wykrywanie niesprawności i błędów w transmisji). Odmiennie niż w NRM wszystkie stacje sieci, tj. główna i podległe, uzyskują w fazie przekazu danych dostęp do kanału na zasadach rywalizacji (bez konieczności odebrania indywidualnego zaproszenia). Taki sposób pracy (możliwy w połączeniach wielopunktowych) może prowadzić do kolizji przesyłanych ramek. W związku z tym ARM stosowany jest w zasadzie wyłącznie w połączeniach punkt-punkt. Tryb ARM jest odpowiedni do obsługi łączysty dupleksoowych przenoszących duży ruch.
- **Asynchroniczny Zrównoważony Tryb Pracy (ABM)** - Tryb ten łączy dwie równoprawne stacje posiadające cechy stacji głównej i podległej. Tryb ten stosowany jest wyłącznie dla połączeń punkt-punkt.

Na zakończenie transakcji stacja główna może zażądać od stacji podległych rozłączenia logicznego poprzez przesłanie komendy DISC. Stacje podległe odpowiadają specjalnymi ramkami, tzw. powiadomienia nienumerowanego UA, przed ich rozłączeniem. Protokół HDLC definiuje przy tym dwa tryby rozłączania logicznego stacji.

Tryby te to:

- **Normalny Tryb Rozłączenia** (ang. NDM - *Normal Disconnected Mode*) oraz
- **Asynchroniczny Tryb Rozłączenia** (ang. ADM - *Asynchronous Disconnected Mode*).

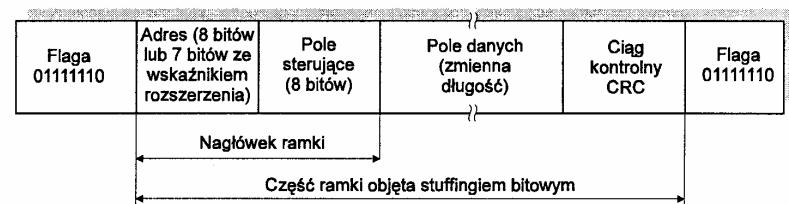
W obu trybach możliwości stacji podległych są ograniczone do zaakceptowania lub odrzucenia komend zarówno ustalających zasady wymiany informacji (ustalających tryb pracy) jak i realizację procesu rozłączenia. Tryby NDM lub ADM definiują więc sposoby reagowania stacji na komendy sterujące w całym okresie przed i po przekazie danych.

ADM różni się przy tym od NDM tym, że oferuje on stacjom podległym możliwość przesyłania ramek żądania nawiązania połączenia logicznego lub inicjowania połączenia ze stacją główną.

W protokole HDLC definiowany jest też tzw. **Tryb Inicjowania Połączenia** (ang. IM - *Initialization Mode*). W trybie tym wymieniane są między stacjami parametry niezbędne do nawiązania połączenia logicznego. Stacja podrzędna wchodzi w tryb IM po odbiorze specjalnej komendy SIM - ustalenia trybu inicjacji (ang. *Set Initialization Mode command*), odpowiadając na nią ramką powiadomienia nienumerowanego UA. Stacja podrzędna może też spowodować wysłanie komendy SIM przez stację główną przesyłając pod jej adresem komendę RIM - żądania trybu inicjacji (ang. *Request Initialization Mode*). W trybie IM stacja może dokonać wstępnej wymiany informacji, pozostając w tym trybie do chwili wejścia w tryb przekazu danych, tj. do przesłania przez stację główną jednej z komend ustalających tryb tego przekazu.

#### 3.5.4 Format ramki

Wiadomości przesyłane zgodnie z protokołem HDLC mają postać ramek o strukturze pokazanej na rysunku 3.12. Wszystkie ramki zaczynają się i kończą ciągami wzorcowymi 01111110 nazywanymi flagami. Ciąg bitów flagi jest ciągiem specjalnym, zastrzeżonym dla celów jednoznacznego ramkowania. Występujące po flagach 8-mio bitowe pole adresu zawiera adres stacji drugiej (odbiorcy bądź stacji podrzędnej), która przesyła bądź też odbiera daną ramkę. Pole danych ramki ma zmienną długość, zależną od długości przesyłanych danych. Zeroową długość tego pola mają ramki sterująco-kontrolne. Jednoznaczność – przeźroczystość - transmisji gwarantowana jest realizowanym przez protokół HDLC stuffingiem bitowym (patrz też SDLC). Dodatkowe bity zerowe (0) generowane po każdym pięciu jedynkach (1) tekstu ramki są usuwane w stacji odbiorczej. Układ odpowiedzialny za generację dodatkowych zer zapewnia też synchronizację bitową w pracy modemów.



Rys. 3.12. Format ramki HDLC

8-mio bitowe lub 16 bitowe, w trybie rozszerzonym (ang. *extended*), pole sterujące definiuje typ ramki oraz rodzaj przenoszonej przez nią komendy/odpowiedzi. Może ono też zawierać numer kolejnego bloku danych przesyłanego i/lub potwierdzanego. Ostatnim polem ramki jest 16-bitowy ciąg kontrolny CRC otrzymywany w wyniku stosowania do celów kodowania wielomianu generującego CCITT-V41.

### 3.5.5 Rodzaje i funkcje ramek stosowanych w HDLC

W protokole HDLC definiowane są trzy rodzaje ramek:

- informacyjne (ang. I - *Information*),
- zarządzające (ang. S - *Supervisory*),
- nienumerowane (ang. U - *Unnumbered*).

Ramki te różnią się strukturą pola sterującego. Różnice między typami ramek ilustruje rysunek 3.13. Wielkość N(s) stanowi numer (modulo 8) ramki informacyjnej I nadawanej przez stację. Z kolei N(r) jest numerem (modulo 8), kolejnej ramki oczekiwanej przez stację. N(r) wskazuje, że wszystkie ramki o numerach N(r)-1 zostały odebrane poprawnie. Bit P/F oznaczający pytanie/kończenie transmisji (poll/final) ma następującą interpretację.

	1	2	3	4	5	6	7	8
Ramka informacyjna (I)	0		N (s)		P/F		N (r)	
Ramka zarządzająca (S)	1	0		Funkcje zarządzania		P/F		N (r)
Ramka nienumerowana (U)	1	1		Specjalizowane funkcje sterujące HDLC		P/F	Specjalizowane funkcje sterujące HDLC	

Rys. 3.13. Znaczenie poszczególnych bitów pola sterującego (8 bitów) w różnych typach ramek HDLC

Wpisanie P/F=1 w przypadku transmisji ramki przez stację główną wskazuje, że stacja ta żąda odpowiedzi stacji podległej. W przypadku ramki nadawanej przez stację podległą ustwienie P/F=1 oznacza zakończenie przez nią odpowiedzi. Rodzaj ramki zarządzającej (nadzorującej) określany jest dwoma bitami pola S. Typy komend przesyłanych w ramkach zarządzających podane są w tabeli 3.3.

Tabela 3.3. Ramki zarządzające S w HDLC

Symbol	Pole sterujące								Funkcja	
	1	2	3	4	5	6	7	8		
RR	1	0	0	0	P/F	N(r)	gotowość do odbioru			
REJ	1	0	0	1	P/F	N(r)	odrzucenie (ramki/ramek)			
RNR	1	0	1	0	P/F	N(r)	brak gotowości do odbioru			
SREJ	1	0	1	1	P/F	N(r)	odrzucenie selektywne ramki			

Ramki zarządzające mogą, podobnie jak ramki informacyjne, przenosić powiadomienia pozytywne o N(r)-1 ramkach odebranych bezbłędnie. Poszczególne ramki nadzorujące mają następującą interpretację:

**RR** - gotowość odbioru (*receive ready*).

Ramka ta przenosi informację (ze stacji głównej bądź podległej) o gotowości do odbioru kolejnych ramek I oraz potwierdzenie poprawnego odbioru ramek o numerach do N(r)-1 włącznie.

**REJ** - odrzucenie (*reject*).

Ramka ta potwierdza odbiór ramek o numerach N(r)-1 włącznie oraz żąda retransmisji ramek I począwszy od N(r).

**RNR** - brak gotowości odbioru (*receive not ready*).

Ramka ta potwierdza odbiór ramek do N(r)-1 włącznie i wskazuje na stan chwilowej niezdolności stacji (np. z powodu przepelnienia jej buforów) do odbioru ramek kolejnych.

**SREJ** - selektywne odrzucenie (*selective reject*).

Ramka ta potwierdza ramki I do numeru N(r)-1 włącznie i żąda retransmisji ramki o numerze N(r).

Z interpretacji ramek zarządzających wynika, że REJ jest ramką stosowaną w przypadku realizacji algorytmu GBN, podczas gdy SREJ znajduje zastosowanie w mechanizmie okienkowym z selektywną retransmisją (SR).

Kolejną grupę ramek sterujących stanowią tzw. ramki nienumerowane. Zestawy komend oraz nienumerowanych odpowiedzi zawarte są w tabelach 3.4 i 3.5.

Tabela 3.4. Komendy nienumerowane (ramki U) w HDLC

Symbol	Pole sterujące								Funkcja
	1	2	3	4	5	6	7	8	
SARM	1	1	1	1	P	0	0	0	ustalenie trybu pracy ARM
SNRM	1	1	0	0	P	0	0	1	ustalenie trybu pracy NRM
SABM	1	1	1	1	P	1	0	0	ustalenie trybu pracy ABM
SARME	1	1	1	1	P	0	1	0	ustalenie rozszerzonego trybu ABM
SNRME	1	1	1	1	P	0	1	1	ustalenie rozszerzonego trybu NRM
SABME	1	1	1	1	P	1	1	0	ustalenie rozszerzonego trybu ABM
DISC	1	1	0	0	P	0	1	0	rozłączenie
SIM	1	1	1	0	P	0	0	0	ustalenie typu inicjalizacji
UP	1	1	0	0	P	1	0	0	nienumerowane przepisywanie
UI	1	1	0	0	P	0	0	0	nienumerowana informacja
XID	1	1	1	1	P	1	0	1	wymiana identyfikacji
RSET	1	1	1	1	P	0	0	1	zerowanie

Tabela 3.5. Odpowiedzi nienumerowane (ramki U) w HDLC (c.d.)

Symbol	Pole sterujące								Funkcja
	1	2	3	4	5	6	7	8	
UA	1	1	0	0	F	1	1	0	nienumerowane powiadomienie
CMDR	1	1	1	0	F	0	0	1	odrzucenie komendy
DM	1	1	1	1	F	0	0	0	tryb rozłączenia
RD	1	1	0	0	F	0	1	0	żądanie rozłączenia
RIM	1	1	1	0	F	0	0	0	żądanie trybu inicjalizacji
UI	1	1	0	0	F	0	0	0	nienumerowana informacja
XID	1	1	1	1	F	1	0	1	wymiana identyfikacji

Poniżej podajemy funkcje wybranych ramek nienumerowanych (komend bądź odpowiedzi).

**SNRM (SNRME)** - komenda SNRM przesyłana przez stację główną inicjuje pracę stacji zgodnie z trybem NRM. Komenda SNRME ma identyczne znaczenie z tą różnicą, że rozszerza ona numerację ramek I do 128 i wydłuża pole sterujące (patrz rys. 3.13).

**SARM (SARME)** - komenda ta inicjuje pracę stacji w trybie ARM; jest ona wysyłana przez stację główną.

**SABM (SABME)** - komenda ta inicjuje pracę stacji w trybie ABM.

Prawidłowy odbiór wszystkich ramek-komend ustalających tryb pracy, tj. SNRM (SNRME), SARM (SARME) i SABM (SABME) jest powiadamiany potwierdzeniem nienumerowanym UA.

**DISC** - komenda ta realizuje rozłączenie logiczne stacji. Stacja odbierająca tę komendę odpowiada potwierdzeniem nienumerowanym UA.

**RSET** - komenda jest używana w trybie ABM do wyzerowania pewnych zmiennych stanu stacji. Stacja odpowiada ramką UA.

**FRMR (CMDR)** - ramki te stosowane są w trybach ABM (NRM/ARM) jako odpowiedzi informujące o odrzuceniu wcześniej odebranej komendy i żądającą reiniitalizacji połączenia.

Różne rodzaje ramek zarządzających i nienumerowanych, w zależności od ich zastosowania do sterowania połączeniem logicznym zgodnie z jednym z trybów pracy, tworzą trzy klasy procedur:

- UAC - Procedury przeznaczone dla niezrównoważonego asynchronicznego trybu odpowiedzi
- UNC - Procedury przeznaczone dla niezrównoważonego normalnego trybu odpowiedzi
- BAC - Procedury przeznaczone dla zrównoważonego asynchronicznego trybu odpowiedzi.

### 3.5.6 Fazy w pracy stacji

W pracy stacji dołączanej do sieci możemy wyróżnić sześć faz:

- (a) stan bezczynności, gdy żadne sygnały nie są przez stację przesyłane;
- (b) stan aktywności, w którym przesyłane są flagi lub ramki;
- (c) fazę zestawiania połączenia, w której inicjowane jest połączenie poprzez przesłanie komend ustalających tryb pracy np. SABM lub SARM.
- (d) fazę przekazu danych, podczas której przesyłane są ramki typu I, S lub U.
- (e) fazę zerowania połączenia, tj. jego reiniitalizowania, realizowaną w przypadku pojawienia się błędów nie wykrywanych przez HDLC, w której to fazie następuje ponowne zestawienie połączenia;
- (f) fazę rozłączenia po zakończeniu przekazu danych, w której przesyłana jest komenda rozłączenia.

W fazie przekazu danych, stacja główna mająca do przesłania ramkę I, przesyła ją wraz z kolejnym numerem danych. Jednocześnie uruchamiany jest licznik czasu odliczający time-out. Kopią ramki I przechowywana jest w buforze stacji do chwili, gdy:

- (1) odebrane zostaje powiadomienie ACK ze stacji podległej (dołączone do ramki I)
- (2) odebrana zostaje komenda REJ (ewentualnie SREJ) i przechowywana ramka I zostaje ponownie przesłana
- (3) upływa time-out i ramka jest retransmitowana.

Po odbiorze ramki I stacja podległa sprawdza najpierw CRC (pole zabezpieczenia kodowego). Jeżeli zostaje wykryty błąd ramka jest odrzucona, sprawdzana jest też zgodność numeru ramki z numerem oczekiwany. Wszystkie ramki I odebrane po tej ramce są przez stację ignorowane (zgodnie z realizowanym algorytmem GBN). W ramkach odebranych wykorzystywany jest jedynie numer N(r) z pola sterującego, traktowany jako powiadomienie pozytywne o N(r)-1 ramkach przesyłanych przez daną stację. Odrzucanie ramki I kończy się z chwilą poprawnego odbioru ramki o właściwym numerze.

W przypadku czasowego przeciążenia stacji i niemożności przyjęcia kolejnych ramek I stacja wysyła komendę RNR, ciągle jednakże akceptuje i interpretuje ramki zarządzające S. Stan zajętości (przeciążenia) stacji jest anulowany przez przesłanie komendy RR lub REJ (ew. SREJ).

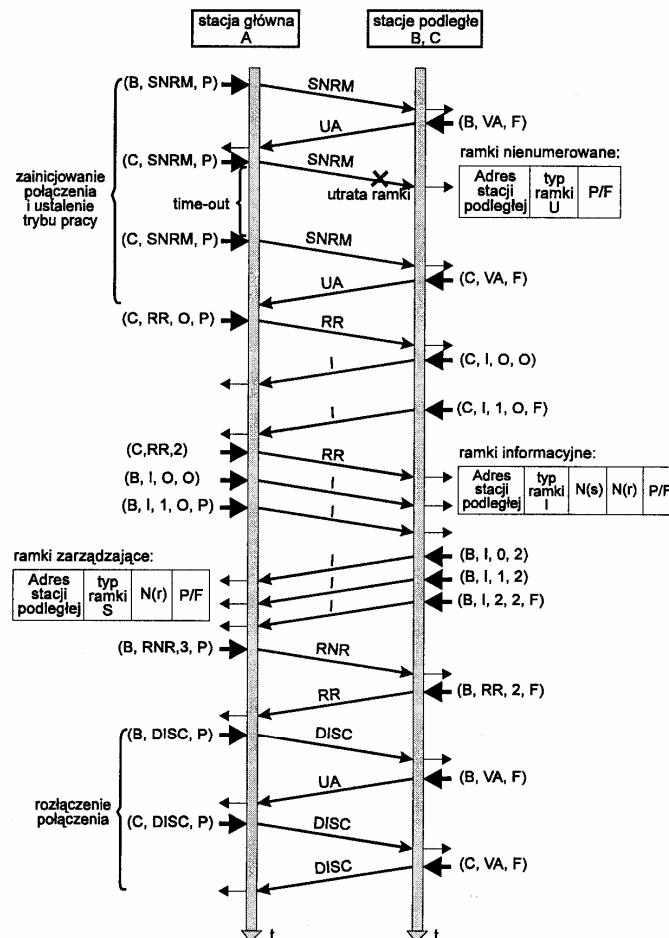
Bity P/F wykorzystywane są do zaproszenia stacji podległych do nadawania (bit P=1) lub przekazania informacji przez stację podległą o zakończeniu transmisji ciągu ramek I (bit F=1).

W implementacjach HDLC dopuszcza się szereg opcji, w ramach których definiowane są podstawowe parametry charakteryzujące pracę stacji. W szczególności są to:

- time-out na retransmisję ramek (do 3 sekund);

- time-out na inicjalizację połączenia (do 90 s.);
- maksymalna liczba bitów informacyjnych w ramce;
- maksymalna liczba transmisji i retransmisji ramki do podjęcia decyzji o zerowaniu połączenia na skutek błędów (do 20);
- szerokość okna (nadawczego).

### 3.5.7 Przykład funkcjonowania HDLC



Rys. 3.14. Przykładowa wymiana ramek pomiędzy stacją główną A, a dwiema stacjami podległymi B i C, zgodnie z trybem NRM: N(s) - numer ostatnio wysłanej ramki I, N(r) - numer kolejnej ramki I oczekiwanej

Ażeby zilustrować realizację procedur HDLC, rozpatrzymy przypadek połączenia wielopunktowego stacji głównej A z dwiema stacjami podległymi B i C. Założymy przy tym, że wymiana informacji pokazana na rysunku 3.14 przebiega zgodnie z trybem NRM.

Komendy i odpowiedzi użyte w diagramie reprezentowane są przez symbole ich nazw. Są one każdorazowo poprzedzone adresem stacji wtórnej (B lub C). Z kolei po symbolu komendy/odpowiedzi mogą występować numery N(s) lub N(r) oraz bity P lub F. Zakładamy, że początkowo kanał jest w stanie nieaktywnym.

W pierwszym kroku stacja A ustala normalny tryb odpowiedzi przesyłając komendę SNRM do stacji podległych B i C. Stacje te potwierdzają odbiór ramki SNRM przesyłając ramki powiadomień nienumerowanych UA. Po zainicjowaniu połączenia i ustaleniu trybu wymiany informacji stacja główna zaprasza stację C do transmisji, przesyłając komendę RR. Stacja C mająca przygotowaną do transmisji wiadomość przesyła dwie ramki I. W ramce kończącej seans łączności ustawia ona bit F=1, oznaczający zakończenie transmisji.

Stacja A potwierdza odbiór tych ramek przesyłając ponownie komendę RR, jednakże z bitem P=0. Oznacza to czasowe zakończenie korespondencji między stacjami A i C.

Z kolei stacja A przesyła dwie ramki do stacji B. Ustawiając w drugiej z nich bit P=1, stacja A oczekuje od stacji B ewentualnego przesłania ramki I lub S z potwierdzeniem przesyłanych danych informacyjnych. Stacja B odpowiada przesyłając 3 kolejne ramki I. W ostatniej z nich ustawia bit F=1, kończąc tę fazę wymiany informacji. Stacja A potwierdza trzy ramki przesyłając do B komendę RNR; oznacza to decyzję o czasowym wstrzymaniu transmisji.

W kolejnym kroku stacja główna inicjuje proces rozłączenia kanału logicznego przesyłając do stacji B i C komendy rozłączenia DISC. Po potwierdzeniu odbioru tej komendy odpowiedziami UA połączenie zostaje zakończone, a kanał zwolniony.

### 3.5.8 Sterowanie przepływem i wykrywanie błędnych ramek

Sterowanie przepływem ramek realizowane jest przez mechanizm okienkowy, określający dopuszczalną liczbę niepotwierdzonych ramek. Liczba ta musi przy tym uwzględniać możliwości stacji do przechowywania kopii ramek oraz opóźnienie propagacyjne w łączu. W przypadku numerowania kolejnych ramek I zgodnie z zasadą modulo 8 (używaną powszechnie w HDLC) możliwe jest teoretycznie przesłanie do 7-mu niepotwierdzonych ramek. W przypadku rozszerzonego trybu pracy SARME, SNRME lub SABME (E-extended mode) rameki są numerowane od 0 do 127 (modulo 128). Oznacza to możliwość przesłania do 127 niepotwierdzonych ramek I.

Ażeby wyeliminować ramki nieprawidłowe, w szczególności o złym formacie, HDLC ma wbudowane procedury kontrolne. Wszystkie ramki zawierające mniej niż 32 bity są przez protokół odrzucone. Stacja nadająca może też spowodować anulowanie w stacji odbiorczej wszystkich ciągów binarnych odebranych po

ostatniej fladze. Do tego celu służy specjalny ciąg wzorcowy składający się z 0 i przynajmniej 7 kolejnych jedynek (od 7 do 14).

Transmisja ciągu jedynek dłuższego niż 14 powoduje natomiast przejście do stanu bezczynności w pracy stacji (łącza). Transmisja tego ciągu sygnalizuje nie-sprawność łącza.

Detekcja pewnych stanów w pracy łącza (stacji) powoduje inicjowanie procedur warstw wyższych. Procedury te wywołują realizację komend utrzymywanych. Ogólnie można stwierdzić, że protokół HDLC jest odporny (ang. *robust*) na różne stany patologiczne, w szczególności w znacznym stopniu eliminuje on, dzięki komendzie RNR, powstawanie zakleszczeń. Jednakże utrata ramki RNR może doprowadzić do zablokowania systemu.

Wszystkie pola ramek, z wyjątkiem flag, zabezpieczane są kodem cyklicznym generowanym zazwyczaj przez wielomian CRC V41 o postaci

$$x^{16} + x^{12} + x^5 + 1,$$

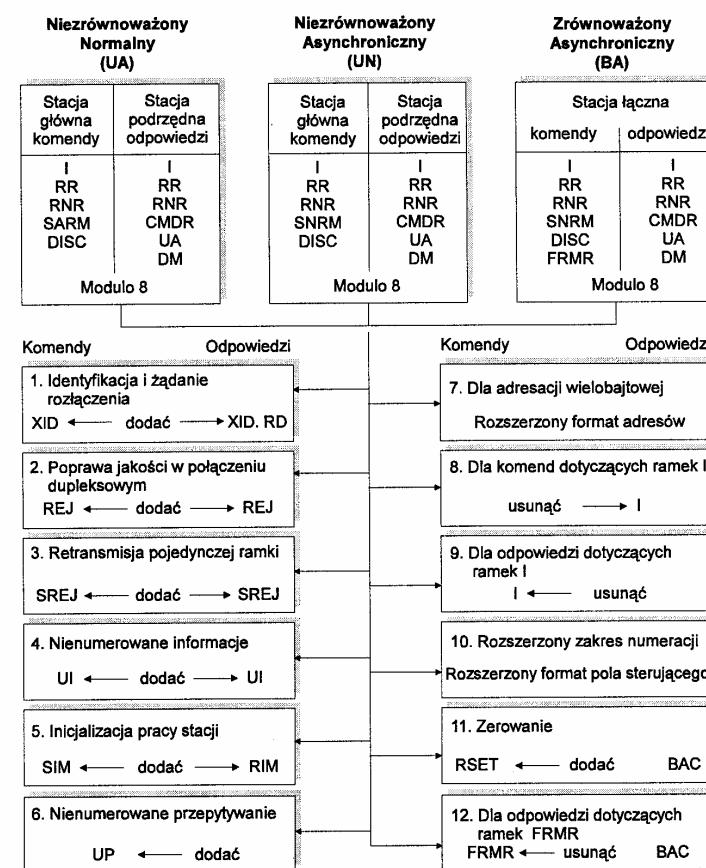
zalecanym przez CCIT. Jednocześnie trzeba podkreślić, że dwa inne wielomiany CRC, a mianowicie  $CRC-12 = x^{12} + x^{11} + x^3 + x^2 + x^1 + 1$  oraz  $CRC-16 = x^{16} + x^{15} + x^2 + 1$  zyskały również miano wielomianów standardowych. CRC-12 używany jest w przypadku, gdy w ramce stosowane są znaki 6-cio bitowe. Z kolei wielomiany CRC-16 i CRC-CCITT znajdują zastosowanie przy zabezpieczaniu znaków 8-mio bitowych. Kody CRC są szczególnie przydatne w przypadku pojawiania się zakłóceń seryjnych. Standardowe ciągi CRC-16 i CRC-CCITT wykrywają wszystkie ciągi błędów (paczki) o długościach 16 bitów lub krótszych, a ponadto 99,997% serii 17-sto bitowych oraz 99,998% ciągów 18-sto bitowych i dłuższych. Ciąg błędów to sekwencja zaczynająca się i kończąca elementami błędymi, wewnętrz której mogą występować elementy (bity) błędne bądź bez błędne. Kody CRC-16 (CRC-CCITT) są również wykorzystywane do zabezpieczania ramek przed błędami niezależnymi. Należy zwrócić uwagę na fakt, że zarówno wyznaczanie sum kontrolnych jak i weryfikacja ich poprawności realizowane są najczęściej sprzętowo z wykorzystaniem prostych rejestrów przesuwowych, co istotnie przyspiesza proces detekcji błędów. Jednocześnie trzeba podkreślić, że z uwagi na brak zabezpieczenia flag w protokole HDLC nawet pojedyncze błędy w ich ciągach mogą poważnie zakłócić prawidłowy przekaz danych. Jeżeli pojedyncze błędy we fladze przekształcają ją w inny ciąg bitów, wówczas rama nie zostanie rozpoznana i mechanizm retransmisji spowoduje ponowne jej przesłanie. Z punktu widzenia funkcjonowania protokołu groźniejsze są jednakże przypadki, gdy błędy wewnętrz ramki powodują, że rozpoznany zostaje ciąg charakterystyczny flagi. Jeżeli dodatkowo kontrola CRC daje wynik prawidłowy, wówczas powstaje błąd niewykrywalny. Błędy flag mogą mieć również wpływ na niewłaściwą interpretację długości odebranej ramki. Gdyby długości ramek były znane (jak np. w DDCMP) błędy takie byłyby wykrywalne. W HDLC jednakże długość ramki jest dowolna. Zwrómy przy tym uwagę na

### 3.5 Protokół bitowy HDLC

fakt, że omawiany poprzednio protokół SDLC zapewniał możliwość wykrywania pewnych błędów flag poprzez sprawdzanie, czy długość ramki jest wielokrotnością liczbą 8.

#### 3.5.9 Klasyfikacja protokołów typu HDLC

Standard HDLC specyfikuje bardzo szeroki zestaw zasad przesyłania informacji na poziomie warstwy łącza danych modelu ISO. Jest rzeczą znamienią, że z uwagi na rozbudowaną strukturę protokół ten nie został w pełni zaimplementowany w żadnym z funkcjonujących systemów komunikacyjnych. Okazuje się, że do poprawnej transmisji danych wystarczy wybrać tylko niektóre elementy protokołu HDLC i w oparciu o nie stworzyć rzeczywisty protokół.



Rys. 3.15. Schemat opcji HDLC

W ten sposób, na podstawie standardu HDLC zostało zdefiniowanych wiele protokołów. Z HDLC wywodzą się między innymi standardy: LLC (protokół kanału logicznego w sieciach lokalnych), LAPB (standard X.25), LAPD (protokół stosowany w sieci ISDN).

Pełna definicja HDLC znajduje się w normach ISO 3309 i ISO 4335 (oraz w dokumentach uzupełniających 7809, 8471, 8885). ANSI ustaliło swoją wersję HDLC i nazwało ją ADCCP. Jest ona zdefiniowana w normie ANSI X3.66. Standard ADCCP różni się od HDLC jedynie szczegółami. Również wiele firm stworzyło swoje własne wersje HDLC, zawierające dodatkowe rozszerzenia. Propozycje klasyfikacji protokołów wywodzących się z HDLC przedstawia rysunek 3.15. Zgodnie z opisem zawartym na rysunku np. oznaczenie UN 3,7 oznacza protokół wywodzący się z HDLC pracujący w trybie *Unbalanced Normal Response Mode* z rozszerzonym polem adresowym i selektywnym żądaniem retransmisji zagubionych (uszkodzonych) ramek.

Jak widać z rysunku 3.15 HDLC przewiduje szeroki zakres realizowanych funkcji. Naturalnym jest więc, że w jednej konkretnej implementacji nie są zrealizowane wszystkie dostępne funkcje. Wybór zależy od projektanta i potrzeb konkretnego zastosowania. Wynika z tego również to, iż produkt jednego producenta HDLC może nie współpracować z protokołem HDLC innego wytwórcy.

#### **LLC**

*Logical Link Control* (LLC) jest standardem firmowanym przez Komitet Standardyzacyjny IEEE 802. Pozwala on na sterowanie przepływem ramek w sieciach LAN (choć jest też możliwe jego wykorzystanie w sieciach rozległych). W klasyfikacji zawartej na rysunku 3.15 protokół LLC oznaczany jest jako BA 2,4. LLC pozwala na realizację trzech wersji implementacji HDLC:

- LLC1 (usługi bezpołączeniowe i bez powiadamiania) z użyciem ramek nienumerowanych UI,
- LLC2 (usługi połączeniowe z potwierdzeniami) z użyciem konwencjonalnych ramek informacyjnych I,
- LLC3 (usługi bezpołączeniowe z potwierdzeniami).

LLC został zaprojektowany do pracy w sieci wielopunktowej z równoprawnymi stacjami (ang. *peer-to-peer*). Dlatego też każda ramka zawiera zarówno adres odbiorcy jak i nadawcy.

#### **LAP**

*Link Access Procedure* (LAP) jest najwcześniej zdefiniowanym podzioborem HDLC. Protokół ten wykorzystuje tryb pracy ARM i niezrównoważoną konfigurację pracy stacji. Możemy go zakwalifikować jako UA 2,8 mimo, iż nie używa ramki DM Response. Protokół ten wykorzystywany jest w niektórych wcześniejszych implementacjach protokołu X.25.

Aby zapoczątkować transmisję zgodnie z protokołem LAP, stacja nadająca wysyła do stacji odbierającej komendę SARM i ustawia *timer T1*. Stacja odbierająca po rozpoznaniu komendy SARM przesyła potwierdzenie, transmitując ramkę UA. W odpowiedzi na przyjście ramki UA stacja nadająca zeruje zegar T1 i ustawia odpowiedni kierunek transmisji. Rozpoznanie, przez stację odbierającą, komendy SARM jest znakiem, że stacja nadająca żąda zmiany kierunku transmisji.

#### **LAPB**

Procedura *Link Access Procedure Balanced* (LAPB) jest powszechnie używana w wielu prywatnych i publicznych sieciach komputerowych na całym świecie. LAPB jest sklasyfikowana jako BA 2,8 lub BA 2,8,10.

Opcja 2 umożliwia równoczesne powtarzanie znieksztalconych ramek w transmisji dwukierunkowej.

Opcja 8 nie pozwala na transmisję danych w ramkach będących odpowiedziami (ang. *response*). To ograniczenie nie jest jednakże problemem, gdyż informacje można przesyłać w ramkach komend, a obie stacje są typu łącznego (ang. *combined*) i obie mogą nadawać komendy. W LAPB ustawienie bitu P=1 oznacza, że stacja żąda ramki statusowej, a nie chce ramki informacyjnej. W konsekwencji nie oczekuje się, że stacja odpowiadająca umieści pole informacyjne w ramce odpowiedzi.

#### **LAPD**

Procedura *Link Access Procedure on the D channel* (LAPD) wywodzi się z LAPB i jest używana w sieciach ISDN. LAPD jest sklasyfikowana jako BA 2, 4, 7, 8, 10.

LAPD zezwala na łączenie się DTE (ang. *Data Terminal Equipment*) z innymi DTE (czyli terminalami) poprzez kanał ISDN D.

LAPD różni się od LAPB przede wszystkim tym, że urządzenia stosujące LAPD - pracują w trybie wielopunktowym (ang. *multipoint*), natomiast używające LAPB w trybie punkt-punkt (ang. *point-to-point*).

Inne różnice między tymi procedurami to:

- LAPD i LAPB używają różnych timerów,
- różnią się budową i znaczeniem pola adresowego,
- w LAPD zaimplementowano ramki UI,
- LAPB używa tylko ramek informacyjnych sekwencyjnych.

##### **3.5.9.1 LAPB**

Protokół LAPB został zastosowany w warstwie drugiej protokołu X.25. Stacje na poziomie tej warstwy drugiej są typu łącznego, tzn. mogą wysyłać/odbierać zarówno komendy jak i odpowiedzi. Stacje DTE i DCE pracują w trybie ABM

(ang. *Asynchronous Balanced Mode*), który pozwala na transmisję bez konieczności otrzymania zezwolenia od innych równorzędnych stacji. Na poziomie warstwy drugiej, dane są przesyłane w trybie połączeniowym.

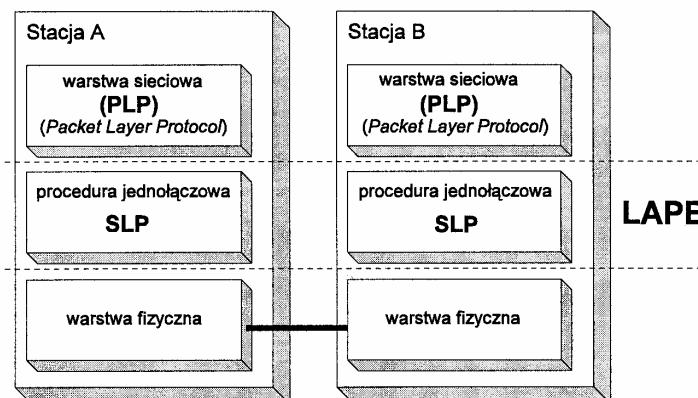
#### • Procedury LAPB

W zależności od liczby utrzymanych połączeń pomiędzy DTE i DCE standard LAPB przewiduje dwa typy procedur:

- procedury jednołączowe SLP (ang. *Single Link Procedure*),
- procedury wielołączowe MLP (ang. *Multiple Link Procedure*).

#### • Procedura jednołączowa (SLP)

Początkowo standard LAPB przewidywał tylko procedurę jednołączową. Procedura ta wykorzystuje jedno łącze fizyczne do przesyłania danych. Miejsce procedury jednołączowej SLP w modelu X25 zostało przedstawione na rysunku 3.16.



Rys. 3.16. Procedury jednołączowe SLP w modelu standardu X.25

Dane na poziomie warstwy WŁD są przesyłane w trybie połączeniowym (w trakcie transmisji możemy więc wyróżnić fazę nawiązania połączenia, fazę przesyłania danych i fazę rozłączenia).

W fazie przesyłania danych, do sterowania przepływem ramek, stacje stosują mechanizm przesuwnego okna. Szerokość okna po stronie nadawczej jest zmieniona i jest określana przez parametr wewnętrzny stacji. Szerokość okna po stronie odbiorczej wynosi zawsze 1 (stosowany jest protokół ARQ typu GoBackN).

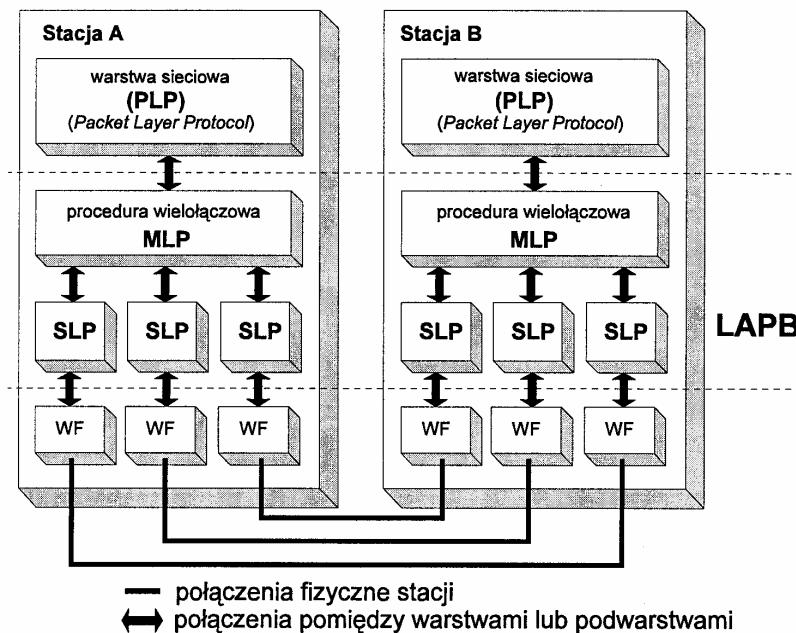
#### Parametry wewnętrzne stacji

Zmienne wewnętrzne stacji zdefiniowane w standardzie LAPB dla procedury jednołączowej to:

T1	(ang. <i>Timer</i> ) służy do odmierzania czasu, w ciągu którego stacja czeka na potwierdzenie ramki i gdy ono nie nadjejdzie, a czas odmierzany przez T1 upłynie, stacja powinna powtórzyć operację nadania ramki.
T2	Maksymalny czas na przygotowanie i wysłanie informacji.
T3	Parametr związany z kontrolą czy kanał jest w stanie jałowym. Parametr nie jest wykorzystywany na poziomie łącza danych.
N1	Maksymalna liczba bitów w ramce informacyjnej.
N2	Parametr określający maksymalną liczbę niedanych prób przesłania ramki. Parametr wykorzystywany i obsługiwany na poziomie warstwy łącza danych. Parametr używany jest w połączaniu z zegarem czasu T1.
k	Maksymalna liczba zaledwych ramek informacyjnych określa szerokość okna protokołu po stronie nadawczej.

#### • Procedura wielołączowa (MLP)

Procedura MLP została wprowadzona do standardu X25 w 1984. Pozwala ona na stosowanie wielu łącz fizycznych do przesyłania danych.



Rys. 3.17. Procedury wielołączowe w standardzie X.25

W przypadku procedury wielołączowej (MLP) możemy wyróżnić dwie podwarstwy: podwarstwę wyższą procedury wielołączowej i podwarstwę niższą zawierającą wiele procedur jednołączowych (patrz rysunek 3.17). Liczba procedur jednołączowych jest równa liczbie posiadanych łącz fizycznych. Procedura wielołączowa realizuje transmisję danych wykorzystując procedury jednołączowe do przesyłania informacji przez łączce fizyczne. Procedury jednołączowe pracujące w ramach stacji działają niezależnie od siebie. Pozwala to na bezpieczniejsze prowadzenie transmisji, gdyż nawet w przypadku uszkodzenia jednego z łącz, dane mogą być przekazywane przez pozostałe łączę.

Procedura wielołączowa, podobnie jak jednołączowa, jest realizowana w trybie połączeniowym z wykorzystaniem mechanizmu przesuwnego okna.

#### **Postać ramki**

Postać ramki LAPB jest zgodna z postacią ramki standardu HDLC. Rozpoczyna się ona polem flagi, po którym następuje pole adresowe (8 bitów), pole kontrolne (8 lub 16 bitów), pole informacyjne (jeśli dany typ ramki dopuszcza pole informacyjne), pole sumy kontrolnej (FCS) i kończące ramkę, pole flagi. Do wyznaczenia sumy kontrolnej stosowany jest wielomian generujący kodu cyklicznego o postaci:  $x^{16}+x^{12}+x^5+1$ .

#### **Adresowanie stacji**

W standardzie LAPB zdefiniowane są cztery typy adresów służące do identyfikacji ramek. Za pomocą adresu dołączonego do ramki i bitów charakterystycznych służących do rozpoznania, która stacja odbiera czy wysyła ramkę, określa się, czy dana ramka jest komendą, czy odpowiedzią. Oto lista dopuszczalnych adresów (bit podany jako pierwszy ma najmniejszą wagę):

- (11000000)B adres nazywany A - adres dla procedury jednołączowej (SLP),
- (10000000)B adres nazywany B - adres dla procedury jednołączowej (SLP),
- (11110000)B adres nazywany C - adres dla procedury wielołączowej (MLP),
- (11100000)B adres nazywany D - adres dla procedury wielołączowej (MLP).

Ramki z innymi adresami niż podane powyżej będą odrzucone przez stację.

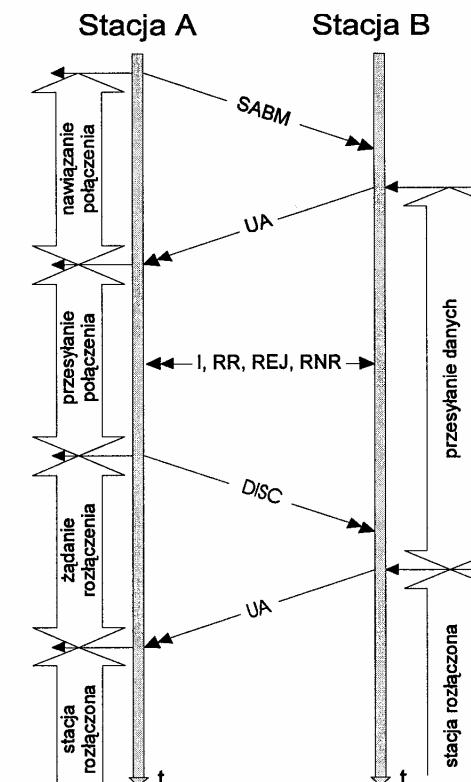
Znaczenie poszczególnych adresów jest przy tym następujące:

- kiedy ramka jest przekazywana od DCE do DTE i zawiera adres A (dla procedury jednołączowej SLP) lub adres C (dla procedury wielołączowej), jest **komendą**.
- kiedy ramka jest przekazywana od DCE do DTE i zawiera adres B (dla procedury jednołączowej SLP) lub adres D (dla procedury wielołączowej), jest **odpowiedzią**.
- kiedy ramka jest przekazywana od DTE do DCE i zawiera adres A (dla procedury jednołączowej SLP) lub adres C (dla procedury wielołączowej), jest **odpowiedzią**.

- kiedy ramka jest przekazywana od DCE do DTE i zawiera adres B (dla procedury jednołączowej SLP) lub adres D (dla procedury wielołączowej), jest **komendą**.

#### **Przebieg transmisji danych w LAPB**

Zgodnie z zaleceniami CCITT stacje są zwykle nazywane odpowiednio: DTE (stacja użytkownika końcowego) lub DCE (zakończenie sieciowe - węzeł sieci). Rysunek 3.18 prezentuje przebieg połączenia zgodnie z protokołem LAPB.



Rys. 3.18. Przebieg połączenia według standardu LAPB

W przykładzie pokazanym na rysunku 3.18 fazy nawiązania i kasowania połączenia są realizowane przez stację A. Fazy te mogą być również realizowane przez stację B. Dozwolona jest też taka sytuacja, że jedna ze stacji nawiązuje połączenie, a druga je rozwiązuje.

### 3.5.9.2 LAPD

Protokół LAPD został zdefiniowany z przeznaczeniem do zastosowania w warstwie łącza danych w sieciach ISDN.

Koncepcja sieci ISDN powstała jako odpowiedź na rosnące zapotrzebowanie na jednolity system cyfrowy, zapewniający dostęp do szerokiej gamy usług telekomunikacyjnych. Sieć ISDN oferuje szeroki zestaw usług przy zastosowaniu ograniczonego zbioru standardowych styków abonenckich (ang. *user-network interface*). Umożliwia to zarówno zastosowanie standardowego terminala ISDN, jak też wprowadzenie nowych rodzajów urządzeń końcowych, bez konieczności zmiany zasadniczej struktury systemu.

Wszelkie zagadnienia, związane z sieciami typu ISDN zostały przedstawione w odpowiednich zaleceniach CCITT. Są to zalecenia serii I. Poszczególne zalecenia tej serii dotyczą:

- I.100 - podstawowych koncepcji w zakresie struktury ISDN, terminologii i innych zagadnień ogólnych,
- I.200 - opisu ISDN w aspekcie oferowanych usług,
- I.300 - aspektów sieciowych ISDN,
- I.400 - styków użytkownik - sieć,
- I.500 - styków między sieciami,
- I.600 - zasad utrzymania sieci ISDN.

Zgodnie z ustaleniami zawartymi w zaleceniu I.120, do podstawowych cech sieci ISDN należą:

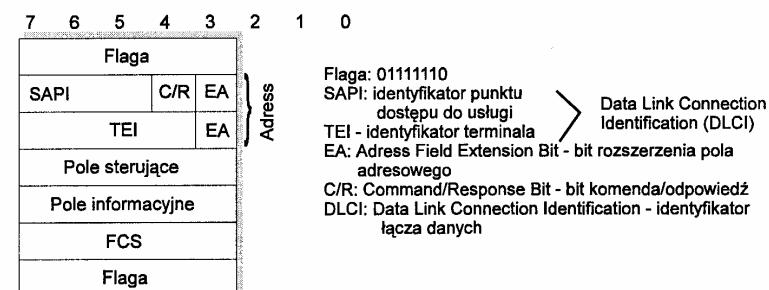
- zapewnianie dostępu do szerokiego zakresu usług fonicznych (usługi typu rozmównego (ang. *voice*), w paśmie telefonicznym) oraz usługi typu non-voice (inne) w ramach jednego systemu, wykorzystując ograniczony zestaw typów połączeń oraz styków użytkownik-sieć,
- zapewnienie realizacji połączeń komutowanych jak i niekomutowanych, przy czym połączenia komutowane obejmują komutację pakietów oraz kanałów (oraz ich połączenia),
- realizację nowych usług z wykorzystaniem cyfrowych połączeń komutowanych o przepływności 64 kb/sek,
- definiowanie układów sterujących realizacją usług, a także zapewniających realizację funkcji utrzymywanych i zarządzania siecią. Dla nowych usług istnieje możliwość wprowadzania dodatkowych układów sterujących w sieci lub terminalach (inteligentne terminale),
- dostęp do ISDN realizowany jest za pomocą protokołów o strukturze warstwowej,
- możliwość implementowania w wielu konfiguracjach, zależnie od wymagań (np. kraju).

### LAPD a HDLC

Procedura LAPD może być zdefiniowana zgodnie z wcześniejszą klasyfikacją (patrz rysunek 3.15) jako opcja HDLC BA 2, 4, 7, 8, 10. Stacje na poziomie warstwy drugiej są typu łącznego (ang. *combined*), co oznacza, że mogą one wysyłać i odbierać zarówno komendy jak i odpowiedzi. Stacje TE i NT pracują w trybie ABME (ang. *Extended Asynchronous Balanced Mode*), który pozwala na transmisję bez otrzymywania zezwolenia od innych równorzędnych stacji; ramki przesypane są przy tym w trybie połączniowym.

#### Struktura ramki

LAPD stosuje ramki bardzo podobne do ramek używanych w HDLC i LAPB (patrz rysunek 3.19). Zastosowanie znajdują więc ramki zarządzające (ang. *supervisory*), nienumerowane (ang. *unnumbered*) i informacyjne (ang. *information*). Stosowana jest też opcja mod 128 umożliwiająca rozszerzoną numerację ramek. W LAPD pole adresowe ma długość dwóch bajtów. Ma to duże znaczenie przy multiplexowaniu wielu funkcji w jednym kanale D. Pole adresowe używane jest zarówno do identyfikacji terminala (ang. *Terminal End-point Identifier* - TEI), jak i punktu dostępu do danej usługi (ang. *Service Access Point Identifier* - SAPI).



Rys. 3.19. Format ramki protokołu LAPD

Z kolei bit EA jest bitem używanym do rozszerzenia pola adresowego. Bit ten ustawiony na 1 oznacza, iż jest to ostatni bajt pola adresowego. W takim przypadku bit o numerze 0 w bajcie drugim (SAPI) musi być równy 0, a bit EA w bajcie trzecim (TEI) równy 1.

Bit C/R wykorzystany jest do rozróżnienia komendy od odpowiedzi. Użytkownik wysyła komendę z bitem C/R=0 a odpowiedź z bitem C/R=1, natomiast system ustanawia znaczenie bitów odwrotnie - komendy z C/R=1, a odpowiedzi z C/R=0.

Pole SAPI identyfikuje adres punktu dostępu do określonej usługi, przez który do punktu dane przesypane są do warstwy wyższej (tj. warstwy sieciowej).

Z kolei TEI identyfikuje połączenie wewnętrz SAPI. TEI umożliwia identyfikowanie do ośmiu pojedynczych lub wielokrotnych terminali.

Pola TEI i SAPI razem tworzą identyfikator łącza DLCI (ang. *Data Link Connection Identifier*), który umożliwia identyfikację każdego połączenia w kanale D.

#### Zarządzanie numerami TEI

Zasadnicza różnica pomiędzy LAPB i LAPD polega na tym, że w LAPD istnieje możliwość podłączenia do "jednego kabla" (łącza fizycznego) wielu terminali. Do rozróżnienia terminali używa się unikatowego, dla każdego urządzenia, numeru TEI.

Definiowane są przy tym dwa rodzaje urządzeń:

- z ręcznie ustawialnym numerem TEI (numerem o wartości od 0 do 63 ustalanym np. za pomocą przełączników).
- z numerem TEI o wartości od 64 do 126 negocjonowanym podczas inicjalizowania pracy urządzenia.

Numer 127 odnosi się do wszystkich terminali.

**Procedura negocjacji numerów TEI** jest przy tym następująca:

Urządzenie LAPD chcąc otrzymać numer TEI wysyła do ASP (ang. *Assignment Source Point*) ramkę nienumerowaną

UI [TEI=127, SAPI=63] <Id rq Ri=x, Ai=y>,

w której y jest żądanym numerem TEI, zaś x jest liczbą wybraną losowo z przedziału <0,65535>. Ustalenie wartości y=127 oznacza, że stacja chce otrzymać jakikolwiek numer TEI. Liczba Ri jest używana do identyfikacji odbieranych ramek - na podstawie tego numeru urządzenie rozpoznaje czy dana ramka dotyczy właśnie tego urządzenia. Jest bardzo mało prawdopodobne, że dwie spośród 126 stacji, jakie mogą pojawić się równocześnie na tym samym kablu (łączu fizycznym), będą miały ten sam numer Ri; Oznaczałoby to, że dwie stacje otrzymały ten sam numer TEI. Aby tego uniknąć zdefiniowano procedurę weryfikacji przydzielonych numerów TEI (patrz poniżej).

Równocześnie z wysłaniem ramki uruchamiany jest zegar T202. Upływ czasu odmierzanego przez ten zegar powoduje konieczność losowania następnej wartości Ri, wysyłanie nowej ramki nienumerowanej

UI [TEI=127, SAPI=63] <Id rq Ri=x, Ai=y>,

i ponowne uruchomienie zegara T202. W przypadku, gdy po upływie określonego czasu urządzenie nie otrzyma numeru TEI uznaje, że otrzymanie numeru TEI jest niemożliwe i przechodzi w stan oczekiwania na dalsze polecenia.

Otrzymanie ramki UI [TEI=127, SAPI=63] <Id ass Ri=x, Ai=y>, w której Ri równe jest wartości Ri w wysłanym żądaniu, oznacza przyznanie numeru TEI=y.

Otrzymanie ramki UI [TEI=127, SAPI=63] <Id den Ri=x, Ai=y>, w której Ri równe jest wartości Ri w wysłanym żądaniu i y<127 oznacza zabronienie używania numeru TEI=y; gdy TEI=127 oznacza to, że nie ma już wolnych numerów TEI. W pierwszym przypadku należy ponowić próbę otrzymania numeru TEI z inną wartością y lub z wartością y=127.

Jeżeli zachodzi podejrzenie, że numery TEI zostały przyznane nieprawidłowo (nie są unikatowe), to wykonywana jest **procedura weryfikacji przyznanych numerów TEI**. Procedura może zostać rozpoczęta albo przez ASP albo przez urządzenie LAPD.

Jeżeli urządzenie chce rozpocząć procedurę weryfikacji, to wysyła do ASP ramkę UI [TEI=127, SAPI=63] <Id vfy Ri=0, Ai=y>, gdzie y jest równe wartości TEI podlegającej weryfikacji. Po odebraniu przez ASP takiej ramki wysyła ono ramkę UI [TEI=127, SAPI=63] <Id chk rq Ri=0, Ai=y>, a wszystkie stacje, które mają przyznanym ten numer TEI muszą odpowiedzieć ramką UI [TEI=127, SAPI=63] <Id chk rq Ri=x, Ai=y> podając nowy numer Ri i swoje TEI (pole Ai). Jeżeli odpowiedzi takich jest więcej niż jedna oznacza to, że numery TEI nie są unikatowe i ASP rozpoczyna opisaną poniżej procedurę usuwania numerów TEI (wszystkich lub tylko tego, który okazał się nie być unikatowy).

Jeżeli ASP podejrzewa niespójność w przyznanych numerach, TEI może sprawdzić wszystkie przyznanego numery TEI. W tym celu wysyła ramkę UI [TEI=127, SAPI=63] <Id chk rq Ri=0, Ai=127>, a wszystkie stacje, muszą odpowiedzieć ramką UI [TEI=127, SAPI=63] <Id chk rq Ri=x, Ai=y>, podając nowy numer Ri i w polu Ai swoje TEI. Jeżeli wśród takich odpowiedzi jest więcej niż jedna z danym numerem TEI oznacza to, że numery TEI nie są unikatowe i ASP rozpoczyna opisaną poniżej procedurę usuwania numerów TEI (wszystkich lub tylko tego, który okazał się nie być unikatowy).

**Procedurę usuwania numerów TEI** rozpoczyna ASP wysyłając ramkę UI [TEI=127, SAPI=63] <Id rmv Ri=0, Ai=y>. Jeżeli y=127 oznacza to żądanie usunięcia wszystkich numerów TEI, w przeciwnym wypadku (y<127) jest to żądanie usunięcia konkretnego numeru TEI. Stacja, która odbierze taką ramkę, przechodzi do stanu początkowego (1.0 wg CCITT), bez względu na to, czy była w trakcie połączenia czy też nie.

## 4 Przewodowe sieci LAN i MAN

Pod pojęciem lokalnej sieci komputerowej LAN (ang. LAN - *Local Area Network*) rozumiemy zespół różnorodnych urządzeń końcowych (w tym komputerów osobistych, serwerów, drukarek, ploterów itp.) połączonych wspólnym medium komunikacyjnym i realizujących zwykle zdecentralizowany algorytm dostępu do tego medium. W przypadku sieci LAN mamy do czynienia z niewielkim obszarem funkcjonowania, ograniczonym zwykle do promienia kilku kilometrów i obejmującym budynek lub zespół budynków jednej instytucji; w przeciwieństwie do sieci rozległej WAN, gdzie wiele instytucji współużytkuje sieć i ma wpływ na jej funkcjonowanie.

Przypadek pośredni między sieciami LAN i WAN, w sensie rozległości terytorialnej, stanowią sieci metropolitalne (ang. MAN - *Metropolitan Area Networks*) pokrywające obszary o promieniu rzędu kilkudziesięciu kilometrów.

*Cechą charakterystyczną zarówno sieci LAN, MAN jak i rozległych sieci satelitarnych jest wykorzystanie do transmisji danych mediów propagacyjnych (przewodowych i bezprzewodowych) pozwalających na realizację wielodostępu na zasadach rywalizacji bądź w oparciu o rozproszone algorytmy tokenowe, czy też procedury rezerwacji. Ponadto w sieciach tych procesy sterowania przepływem informacji w warstwie WŁD są rozdzielone od zagadnień dostępu do medium.*

Sieci satelitarne możemy traktować jako sieci o topologii gwiaździstej, w których wymiana informacji między stacjami realizowana jest za pośrednictwem prze-kaźnika mikrofalowego umieszczonego na satelicie (np. geostacjonarnym).

W dwóch pierwszych typach sieci, tj. sieciach LAN i MAN

- szybkości transmisji są zwykle dużo większe od realizowanych w sieciach rozległych WAN z transmisją typu punkt-punkt, a
- elementowa stopa błędów w kanałach tych sieci jest z kolei znacznie mniejsza od średnich wartości uzyskiwanych w sieciach WAN.

Dominującą rolę wśród wymienionych sieci z medium propagacyjnym odgrywają przewodowe sieci lokalne LAN. Wybrane własności sieci LAN dostępnych na rynku ilustruje tabela 4.1.

Główne przyczyny tworzenia tych sieci i ich ciągła i duża atrakcyjność wynikają z:

- możliwości zapewnienia użytkownikom dostępu do kilku (kilkunastu) komputerów danej instytucji,
- współużytkowania zbiorów,
- współużytkowania pamięci operacyjnych, pamięci masowych i drukarek przez proste stacje końcowe użytkowników,

- wykorzystania wspólnych urządzeń pośredniczących w dostępie do sieci rozległych,
- zapewnienia nowych usług, w tym poczty elektronicznej, użytkownikom sieci.

Tabela 4.1. Podstawowe parametry wybranych sieci LAN

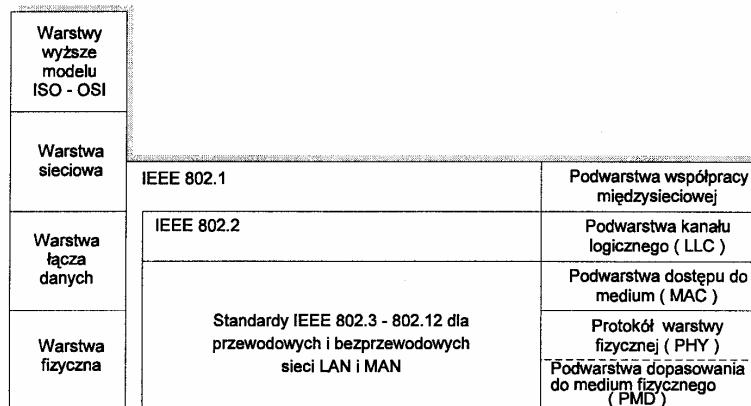
Nazwa	Topologia	Rodzaj medium	Szybkość transmisji	Metoda dostępu	Maksymalna długość segmentu/sieci	Maksymalna liczba stacji
100VGAny-LAN	gwiazda	skrętka 3 kat./ światłowód	100 Mb/s	Dostęp priorytetowy (ramki Ethernet/ Token Ring)	150/segment dla skrętki 5 kat.	zalecenia 250 (1024)
AppleTalk/ LocalTalk	magistrala	skrętka	0.23 Mb/s	CSMA/CD	330m	32/segment
ARCNet	drzewo	koncentryk/ światłowód/ skrętka	2,5 Mb/s (20 Mb/s)	Token	600/6000m 305m	255
Cambridge Ring	pętla (pierścień)	skrętka	10 Mb/s	Token	ok. 1000m	ok. 100
Ethernet	magistrala	skrętka, koncentryk	10 - 20 Mb/s typowo 10 Mb/s	CSMA/CD	500/2500m	1000/segment
Fast Ethernet	gwiazda/ drzewo	skrętka 5 kat./ światłowód	100 Mb/s	CSMA/CD	412m	
FDDI I	pętla/ pierścień	światłowód	100 Mb/s	Token	do 200 km	1000 (praktycznie nieograniczona)
FDDI II	pętla (pierścień)	światłowód	100 Mb/s	Token/ rezerwacja	do 200 km	1000 (praktycznie nieograniczona)
IBM Token Ring	pętla (pierścień)	skrętka, światłowód	4/16 Mb/s	Token	200/2000m	260
ISO Ethernet	gwiazda/ drzewo	skrętka/ światłowód	max. 16.364	definiowane różne tryby pracy ustalane podczas autonegoacji	100m	
DECNet (Ethernet)	magistrala/ drzewo	koncentryk	10 Mb/s	CSMA/Cd	500/2800m	1000/segment

Małe odległości między stacjami bądź też stosowanie kabli światłowodowych (w szczególności światłowodów jednomodowych) pozwala na uzyskiwanie w sieciach LAN i MAN szybkości transmisji rzędu 100Mb/s (a nawet większych). Mówimy wówczas o szybkich sieciach lokalnych (ang. *High Speed LAN*), lub szybkich sieciach metropolitalnych.

W dalszej części rozdziału przedstawimy podstawowe problemy sterowania przesyaniem ramek informacyjnych w przewodowych sieciach LAN i MAN, tj. zagadnienia funkcjonowania podwarstwy kanału logicznego LLC. W kolejnych paragrafach tego rozdziału i w rozdziale następnym omówimy przykładowe algorytmy pracy podwarstwy MAC, dostępu do medium, stosowane w sieciach LAN i MAN (w tym w sieciach radiowych) oraz rozległych sieciach satelitarnych typu VSAT.

#### 4.1 Podwarstwa kanału logicznego - LLC

Większość funkcjonujących instalacji sieci LAN realizuje zalecenia Komitetu IEEE 802 w odniesieniu do zasad organizacji warstw WF i WŁD oraz wypełnianych przez nie funkcji i świadczonych usług. Zgodnie z koncepcją struktury warstwowej dla sieci LAN standard IEEE 802.2 (lub ISO 8802.2), odnoszący się do podwarstwy LLC, wraz z odpowiednim standardem podwarstwy dostępu do medium MAC (IEEE 802.3 - 802.7, 802.9 oraz 802.11 i 802.12) realizują funkcje przypisane warstwie łącza danych jako całości, w architekturze systemu ISO-OSI (patrz rysunek 4.1).



Rys. 4.1. Ilustracja zależności pomiędzy standardami IEEE 802, a modelem ISO-OSI

**Definiowana przez standard IEEE 802.2 i zunifikowana dla wszystkich sieci LAN podwarstwa kanału logicznego LLC komunikuje się z warstwą sieciową za pośrednictwem zestawu operacji podstawowych - prymitywów LLC. Z kolei komunikacja podwarstwy LLC z podwarstwą MAC dokonywana jest z wykorzystaniem odpowiednich prymitywów MAC.**

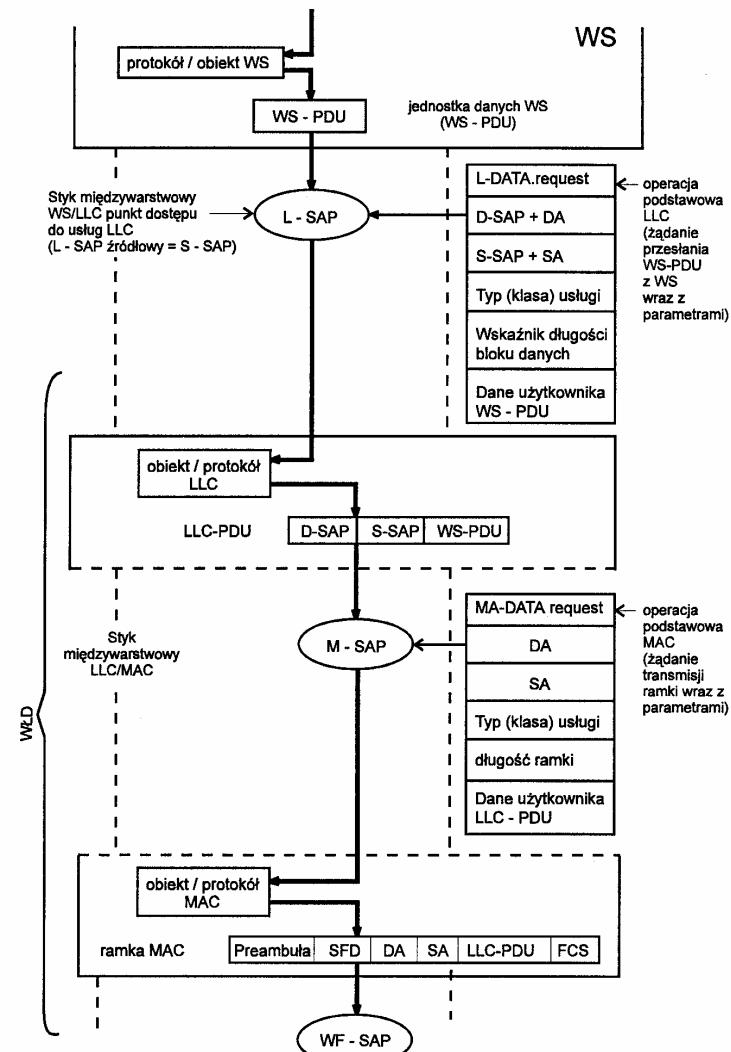
Warstwowy przekaz informacji między obiektem LLC w komunikujących się stacjach sieci odbywa się poprzez wymianę jednostek danych podwarstwy LLC. Możliwe są przy tym trzy typy realizacji tej wymiany, odpowiadające prezentowanym w rozdziale 2 typom usług warstwowych:

- 1) Typ 1 - określany mianem usługi bezpołączeniowej bez potwierdzeń (LLC-1);
- 2) Typ 2 - określany mianem usługi połączeniowej (LLC-2); oraz
- 3) Typ 3 - stanowiący usługę bezpołączeniową z potwierdzeniami (LLC-3).

W typie 1 realizowany jest przekaz informacji do określonej stacji lub grupy stacji (zgodnie z adresem zawartym w ramce MAC). Nie przewiduje się przy tym przesyłania potwierdzeń.

#### 4.1 Podwarstwa kanału logicznego - LLC

Typ 3 określany jest mianem rozszerzonej usługi bezpołączeniowej. W tym typie usługi przewiduje się potwierdzenia, które mogą być przy tym generowane zarówno przez warstwę WŁD (MAC) (np. w IEEE 802.5), jak też warstwę sieciową (w zależności od przyjętej opcji).



Rys. 4.2. Ilustracja organizacji warstwy WŁD i zasad współpracy WŁD z WS, w przypadku przepływu informacji z WS

W przypadku typu 2 (LLC-2) wykorzystywany jest szeroki zestaw operacji podstawowych umożliwiających zestawienie połączenia, wymianę informacji oraz dokonywanie rozłączenia, a także zerowanie połączenia i sterowanie przepływem ramek. Realizowane też mogą być różne klasy usług, uwzględniające priorytety w wymianie informacji, o ile możliwości takie są dostępne w określonej sieci LAN.

Zgodnie z modelem warstwowy dla sieci lokalnej *usługi transportowe oferowane przez podwarstwę LLC są udostępniane użytkownikowi (warstwie wyższej) poprzez jeden lub więcej tzw. punktów dostępu do usług* (ang. SAP - Service Access Point) tworzących logiczny styk między sąsiadującymi warstwami (por. rysunek 4.2). Poszczególne punkty dostępu do usług świadczonych przez LLC, (L-SAP) są zwykle związane z różnymi protokołami warstw wyższych, a tym samym z różnymi aplikacjami.

Tabela 4.2. Zestawienie operacji podstawowych LLC dla różnych typów usług

Typ 1 usługi bezpołączeniowe bez potwierdzeń	L-UNIDATA.request L-UNIDATA.indication
Typ 2 usługi połączeniowe	L-CONNECT.request L-CONNECT.indication L-CONNECT.response L-CONNECT.confirm L-DATA.request L-DATA.indication L-DISCONNECT.request L-DISCONNECT.indication L-RESET.request L-RESET.indication L-RESET.response L-RESET.confirm L-CONNECTION-FLOWCONTROL.request L-CONNECTION-FLOWCONTROL.indication
Typ 3 usługi bezpołączeniowe z potwierdzeniami	L-DATA-ACK.request L-DATA-ACK.indication L-DATA-ACK-STATUS.indication L-REPLY.request L-REPLY.indication L-REPLY-STATUS.indication L-REPLY-UPDATE.request L-REPLY-UPDATE-STATUS.indication

**Egzekwowanie i sterowanie przebiegiem wykonania różnych typów usług odbywa się za pośrednictwem operacji (prymitywów LLC).** Zestawy tych prymitywów dla poszczególnych typów usług są zawarte w tabeli 4.2.

**Prymitywy te mogą być realizowane jako przerwania lub wywoływanie procedur z odpowiednimi parametrami.** Parametrami operacji podstawowych mogą przy tym być: dane do przesłania, adresy, priorytety czy też typy usług.

Należy podkreślić fakt, że standardowy protokół podwarstwy LLC może współpracować z dowolnym protokołem podwarstwy MAC serii IEEE 802. Styk międzywarstwowy LLC/MAC definiują, zgodnie ze standardem IEEE trzy prymitywy. Są to:

MA-DATA.request,

MA-DATA.confirm oraz

MA-DATA.indication.

Przykład współpracy międzywarstwowej WS/LLC oraz LLC/MAC ilustruje rysunek 4.2. Na rysunku tym pokazano zarówno operacje podstawowe typu DATA.request z ich parametrami, jak też w sposób poglądowy ukazano mechanizm tworzenia ramek: LLC i MAC. Zwróćmy przy tym uwagę na fakt, że warstwa znajdująca się bezpośrednio nad LLC (na rysunku 4.2 warstwa sieciowa) specyfikuje adresy: źródłowy i docelowy jako złożenie odpowiednich adresów punktów dostępu do usług L-SAP (ang. D-SAP - Destination SAP lub S-SAP - Source SAP) oraz adresów fizycznych stacji (ang. DA - Destination Address i SA - Source Address), tj. adresów MAC.

W zależności od rodzajów (typów) usług zaimplementowanych w stacji i oferowanych przez LLC warstwom wyższym definiowane są cztery klasy stacji:

klasa 1 - obejmująca stacje oferujące usługę LLC-1,

klasa 2 - związana ze stacjami realizującymi tryby pracy LLC-1 i LLC-2,

klasa 3-odnosząca się do stacji oferujących tryby pracy bezpołączeniowe LLC-1 i LLC-3 oraz

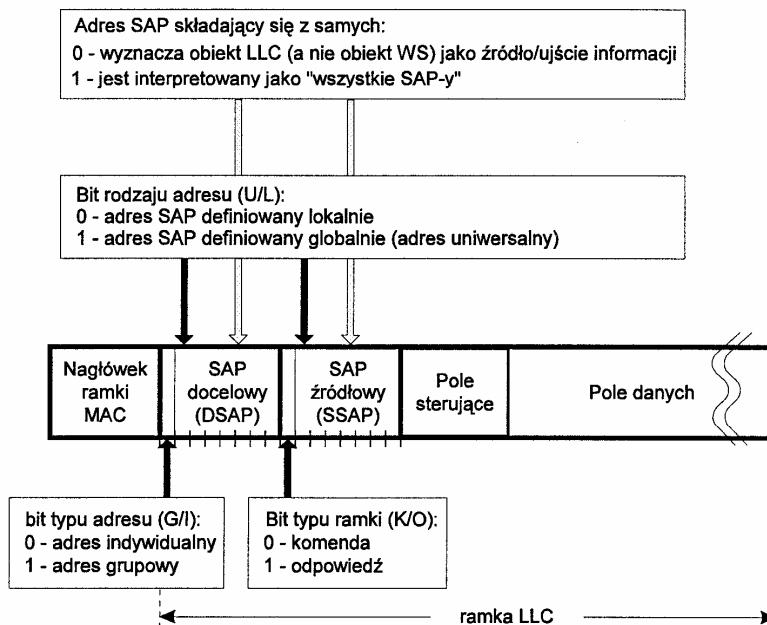
klasa 4 - odpowiadająca stacjom realizującym wszystkie typy usług.

Usługi poszczególnych typów (LLC-1-3) są realizowane w stacji przez protokół podwarstwy LLC sterujący przekazem protokolarnych jednostek danych podwarstwy LLC, przenoszonych poprzez sieć LAN za pośrednictwem ramek MAC. Ramki informacyjne "numerowane" stosowane są w przekazie danych zorientowanym połączeniowo (LLC-2), natomiast tzw. ramki nienumerowane są wykorzystywane w przekazie bezpołączeniowym (typy LLC-1 i LLC-3), nazywanym też usługą datagramową.

Standard LLC IEEE 802.2 jest w znacznym stopniu wzorowany na popularnym protokole WŁD jakim jest protokół bitowy HDLC. LLC IEEE 802.2 nie uwzględnia jednakże struktury ramki definiowanej w HDLC. Analiza przydatności HDLC dla wymiany informacji w sieci LAN wykazała też, że niektóre propo-

nowane przez ten protokół procedury, a w szczególności wtrącania bitów (tzw. stuffing bitowy) i generacji flag są źle dopasowane do potrzeb sieci LAN.

W przypadku sieci LAN adresy stacji źródłowej i docelowej oraz pola kontrolno-sterujące są zawarte na początku ramki MAC. Zawartość pola danych ramki LAN - stanowiącą ramkę przygotowywaną przez podwarstwę LLC - ilustruje rysunek 4.3.



Rys. 4.3. Format ramki LLC

Standard LLC 802.2 może być traktowany jako opcja protokołu HDLC z asynchronicznym zrównoważonym trybem pracy (ang. *Asynchronous Balanced Mode*). W opcji tej w szczególności:

- użyto rozszerzonych formatów (modulo 128) pól numerów sekwenncyjnych ramek,
- wprowadzono 16-bitowe pole adresowe dla adresów punktów dostępu do usług (D-SAP/S-SAP),
- wprowadzono trzy nowe komendy nienumerowane, a mianowicie UI, XID oraz TEST oznaczające odpowiednio: nienumerowany blok danych, blok wymiany parametrów stacji, żądanie przesłania identycznej ramki TEST w celu skontrolowania połączenia LLC-LLC,
- zrezygnowano z użycia komend SREJ oraz CMDR.

Zestawy komend i odpowiedzi tj. zestawy ramek informacyjnych i sterujących protokołu LLC 802.2 odnoszące się do dwóch najpopularniejszych typów usług LLC-1 i LLC-2 oraz najczęściej spotykanych klas stacji, tj. klasy 1 i klasy 2, podane są na rysunku 4.4.

	Typ usługi	Komendy (rozkazy)	Odpowiedzi	Typ ramki
klasa stacji Klasa 2	Typ 1	UI - nienumerowana rama informacyjna XID - wymiana parametrów stacji TEST - żądanie przesłania identycznej ramki TEST	- XID TEST	U
		I - ramka informacyjna	I	I
	Typ 2	RR - gotowość odbioru RNR - brak gotowości odbioru REJ - odrzucenie ramki	RR RNR REJ	S
		SABME - zainicjowanie rozszerzonego trybu ABM DISC - rozbiorzenie	UA - nienumerowane ACK DM - tryb rozłączania FRMR - odrzucenie wcześniejszej komendy	U

Klasa 1 - obsługuje operacje bezpołączeniowe (LLC - 1)

Klasa 2 - obsługuje operacje połączeniowe i bezpołączeniowe (LLC - 1, LLC - 2).

Rys. 4.4. Zestawy komend i odpowiedzi w usługach typu LLC-1 i LLC-2 dla klasy 1 i klasy 2

Wyjaśnienie znaczenia poszczególnych komend i odpowiedzi można znaleźć w rozdziale poświęconym protokołowi HDLC.

Jak wspomnieliśmy poprzednio, stacje klasy 1 zapewniają usługę bezpołączeniową. Ten typ stacji odnosi się głównie do urządzeń pracujących w sieciach IEEE 802.3 - CSMA/CD i IEEE 802.4. Z kolei klasa 2 preferowana jest w IBM-owskich sieciach IEEE 802.5, pozwalających na realizację usług zarówno bezpołączeniowych jak i połączeniowych.

Na zakończenie zwróciśmy też uwagę na fakt, że niektóre komendy (rozkazy) i odpowiedzi, jak to ma miejsce w przypadku ramek XID i TEST, są wyróżnione poprzez ustawienie jednego z bitów w polu adresowym S-SAP; 0 - odpowiada komendzie, podczas gdy 1 - stanowi "informację", że zawartość ramki XID (TEST) niesie odpowiedź (por. rys. 4.3).

#### 4.1.1 Adresy w sieciach LAN

Każde urządzenie w sieci LAN (serwer, stacja robocza, most, router) jest identyfikowane za pomocą adresu fizycznego, określonego też mianem adresu sprzętowego - z uwagi na to, że jest on na stałe związany z płytą główną lub kartą

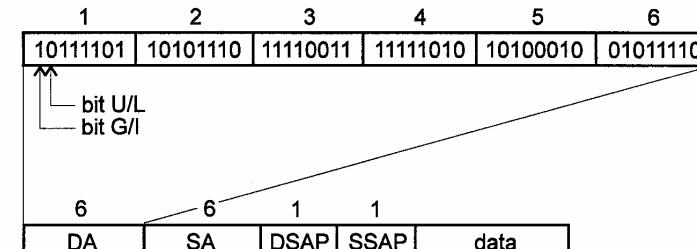
sieciową włączoną do urządzenia. Adres stacji nazywany jest też czasem adresem MAC-owym, z uwagi na jego obecność w ramce przygotowywanej przez podwarstwę MAC. W części organizacyjnej ramki przesyłanej przez sieć są zawarte dwa adresy: adres stacji źródłowej (ang. source address - SA) i adres stacji docelowej (ang. Destination Address - DA). Aby zapobiec zbyt częstym przerwaniom programowym, związanym z odbiorem napływających do stacji ramek, każda karta sieciowa odfiltrowuje adresowane do niej ramki. Operacja filtracji, realizowana w całości sprzętowo, polega na sprawdzeniu:

1. czy adres docelowy DA ramki pokrywa się z adresem fizycznym stacji i przekazaniu ramki do dalszego przetwarzania w stacji w przypadku zgodności adresów, bądź
2. odrzuceniu ramki, gdy zostanie stwierdzona niezgodność.

Ponieważ w sieci pracuje wiele urządzeń, ważne jest aby ich adresy nie pokrywały się. Łatwo to zapewnić w pojedynczej sieci LAN. Jednakże w sieci złożonej z wielu segmentów bądź w przypadku połączonych sieci LAN zagadnienie niepowtarzalności adresów nabiera dużego znaczenia. Dążąc do zapewnienia globalnej jednoznaczności adresów Komitet 802 IEEE dokonał standaryzacji adresów w podlegających standardom IEEE sieciach LAN. Zalecenia IEEE dopuszczały adresy 16-sto bitowe bądź 48-mio bitowe dla sieci LAN, z wyjątkiem standardu 802.6 (DQDB). W tym ostatnim przypadku, z uwagi na przystosowanie do współpracy z sieciami B-ISDN ATM, przewidziano dodatkowo możliwość stosowania adresów 60-cio bitowych. W praktyce adresy 16-sto bitowe nie znajdują szerszego zastosowania (choćż w niektórych przypadkach mają one pewne zalety, dotyczy to np. szybkości rozstrzygania sytuacji konfliktowych pojawiających się w pracy sieci IEEE 802.4). Ogólnie akceptowanym administratorem i dystrybutorem adresów dla sieci LAN jest IEEE. Organizacja ta przyznaje (a dokładniej sprzedaje) producentom sprzętu komputerowego 6-cio bajtowe bloki adresowe. 3 pierwsze bajty każdego z tych bloków (24 bity) mają strukturę określzoną przez IEEE. Pozostałe 3 bajty mogą być zagospodarowane przez producenta, bądź lokalnego administratora sieci LAN. Blok (ciąg bitów) o ustalonej zawartości nazywany jest czasem kodem producenta bądź jednoznacznym identyfikatorem organizacyjnym. Wśród 24 bitów tego ciągu dwa bity, w pierwszym bajcie, oznaczane jako U/L oraz G/I, mają specjalne znaczenie.

Bit U/L (ang. *Universal/Local*) (por. rysunek 4.5) definiuje globalne bądź lokalne znaczenie adresu. Innymi słowy opisuje on, czy:

- karta sieciowa została wyprodukowana z przeznaczeniem do sieci, w której adresy są administrowane globalnie (adresy uniwersalne w całym środowisku połączonych sieci i nadzorowane przez IEEE); U/L=1; czy też:
- karta sieciowa (i adres fizyczny urządzenia) jest wykorzystywana lokalnie; U/L=0.



Rys. 4.5. Struktura adresu

W przypadku przekazania bloku adresowego producentowi bit U/L ustawiany jest jako 1. Jednakże lokalny administrator może dokonać zmiany jego wartości. Drugi ze wspomnianych bitów, tzw. bit G/I (ang. *Group/Individual*) definiuje, czy:

- adres dotyczy pojedynczego urządzenia; G/I=0; czy też:
- grupy urządzeń; G/I=1.

W tym drugim przypadku pod pojęciem grupy urządzeń rozumiemy stacje określonego typu, np. serwery nazw, serwery zbiorów, koncentratory, routery czy też mosty. W sytuacji, gdy stacja robocza chce skorzystać z usługi typu X, wówczas przesyła ramkę z adresem grupowym serwerów X. Adresy grupowe są też często określane mianem adresów multicastowych.

W przypadku połączonych mostami sieci IEEE 802.5 (sieci pętlowych ze znacznikami) ustawienie bitu G/I=1 w adresie źródłowym oznacza, że ramka MAC zawiera dodatkowe informacje o adresach mostów i segmentów sieci LAN, niezbędne do zrealizowania, stosowanej w tym przypadku, metody routingu źródłowego (ang. *source routing*).

Jak wspomnieliśmy wcześniej standard IEEE dopuszcza też adresy 16-sto bitowe. Format ten dotyczy wyłącznie adresów administrowanych lokalnie. Jeden z bitów pola adresowego definiuje wówczas, podobnie jak w adresach 6-cio bajtowych, rodzaj adresu urządzenia, tj. G/I - *Group/Individual*.

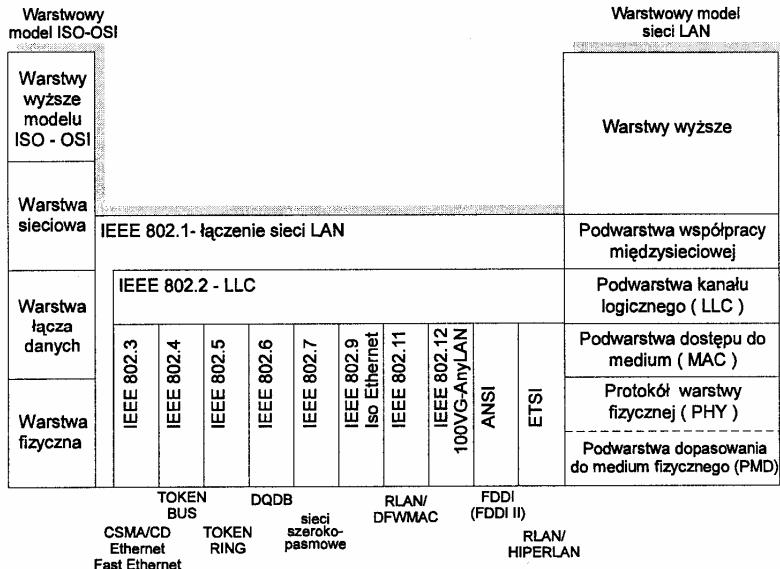
Zwróćmy uwagę na fakt, że warstwa wyższa w stosunku do warstwy WLD w sieciach LAN specyfikuje adresy: źródłowy i docelowy jako złożenie (konkatenację) adresu fizycznego, tj. adresu MAC-owego oraz adresu L-SAP punktu dostępu do usług podwarstwy LLC. W sieciach LAN adresy punktów dostępu są zwykle jednobajtowe. Występują one w odmianie indywidualnej i grupowej (G/I), jak też globalnej i lokalnej (U/L) (patrz rysunek 4.3 i rysunek 4.5).

Ogólnie można przyjąć, że adres L-SAP określa konkretny protokoł warstwy wyższej. Zazwyczaj wiąże się on również z określonym procesem aplikacyjnym. Jeżeli proces ten nie jest przypisany konkretnej stacji fizycznej, to uzasadnione

staje się stosowanie grupowego adresu fizycznego MAC w powiązaniu z indywidualnym adresem L-SAP. Tak więc, gdy sieć LAN potraktujemy jako środowisko do rozproszonego przetwarzania danych to może się okazać, że indywidualne adresy MAC znajdą w tej sieci niewielkie zastosowanie.

## 4.2 Podwarstwa dostępu do medium MAC

Przedstawimy obecnie wybrane protokoły dostępu do medium stosowane w przewodowych sieciach LAN i MAN. Zwrócimy przy tym uwagę na formaty ramek stosowane w różnych sieciach oraz zasady sterowania ich dostępem do medium. Nakreślimy też ogólne zasady zarządzania pracą podwarstwy MAC. W kolejnych paragrafach omówimy całą rodzinę algorytmów przyjętych jako powszechnie akceptowane standardy IEEE, ANSI oraz ETSI. Algorytmy standardowe prezentowane będą w zasadzie w kolejności zgodnej z ich rosnącą numeracją, proponowaną przez IEEE. Ilustruje to rysunek 4.6. Proponowana koncepcja prezentacji ma zarówno zalety jak i wady. Pewnym jej mankamentem jest fakt przemieszczania różnych algorytmów dostępu do medium. Protokoły rywalizacyjne nie będą więc omawiane jako jeden blok systemowy. Częste odwoływanie się do cech charakterystycznych różnych metod dostępu i zarządzania podwarstwą MAC pozwoli jednakże Czytelnikowi na zapoznanie się zarówno z zaletami i postulowanymi zastosowaniami omawianych rozwiązań, jak i z ich wadami i wynikającymi z nich ograniczeniami aplikacyjnymi.

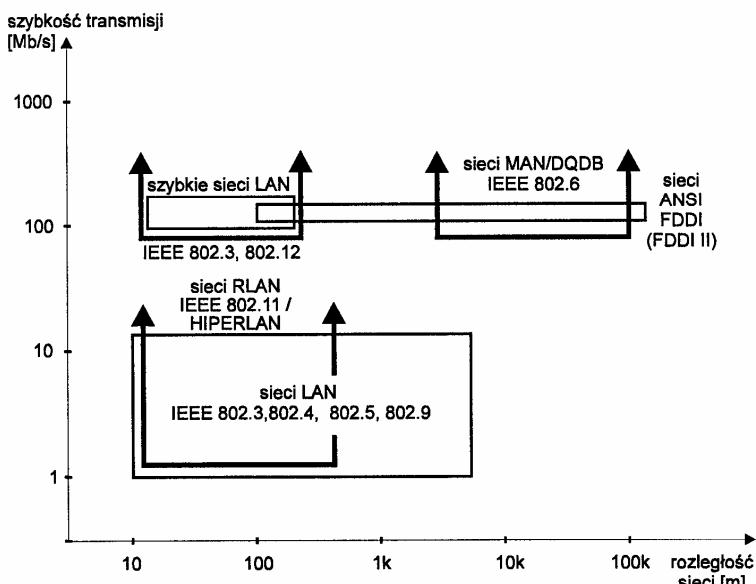


Rys. 4.6. Prezentacja standardów WŁD

W pierwszym paragrafie omówimy najpopularniejszy standard sieci LAN jakim jest CSMA/CD IEEE 802.3. W kolejnych podrozdziałach zaprezentujemy popularne rozwiązania tokenowe IEEE 802.4 i 802.5 dla przewodowych sieci LAN, a także coraz popularniejsze rozwiązania Fast Ethernet, Giga Ethernet oraz 100VGAnyLAN. Opisemy też koncepcję pracy sieci LAN umożliwiającej realizację usług multimedialnych - IsoEthernet IEEE 802.9. Następnie przedstawimy dwa standardy dla sieci metropolitalnych: DQDB IEEE 802.6 i ANSI FDDI.

Propozycje rozwiązań dostępu do medium w sieciach bezprzewodowych (w tym nie będące standardami algorytmy ALOHA i CSMA oraz standardy IEEE 802.11 i ETSI HIPERLAN) oraz sieci VSAT zostaną omówione w następnym, 5-tym rozdziale książki.

Podstawowe parametry większości spośród omawianych dalej rozwiązań sieci LAN i MAN, tj. szybkości transmisji i rozległości terytorialne tych sieci, ilustruje rysunek 4.7.



Rys. 4.7. Klasifikacja sieci LAN, MAN

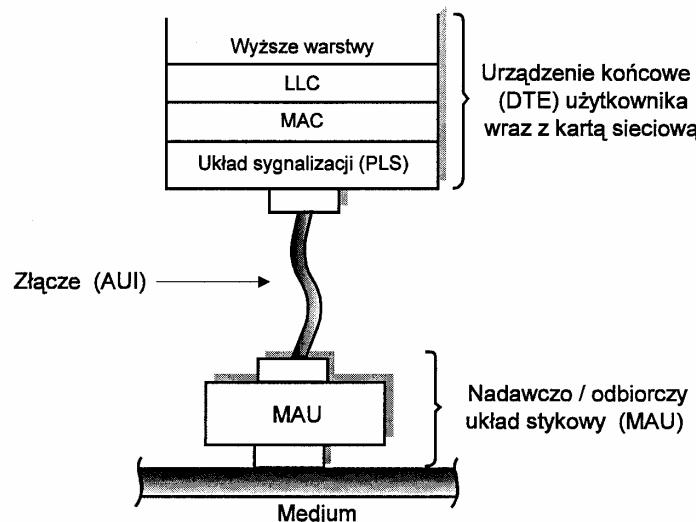
### 4.2.1 Protokół rywalizacyjny CSMA/CD - Standard IEEE 802.3

Standard CSMA/CD IEEE 802.3, opublikowany w 1985r., został opracowany na podstawie dokumentacji sieci Ethernet. Wykorzystuje on protokół CSMA/CD, będący naturalnym rozszerzeniem algorytmu CSMA (ang. *Carrier Sense Multiple Access with Collision Detection*).

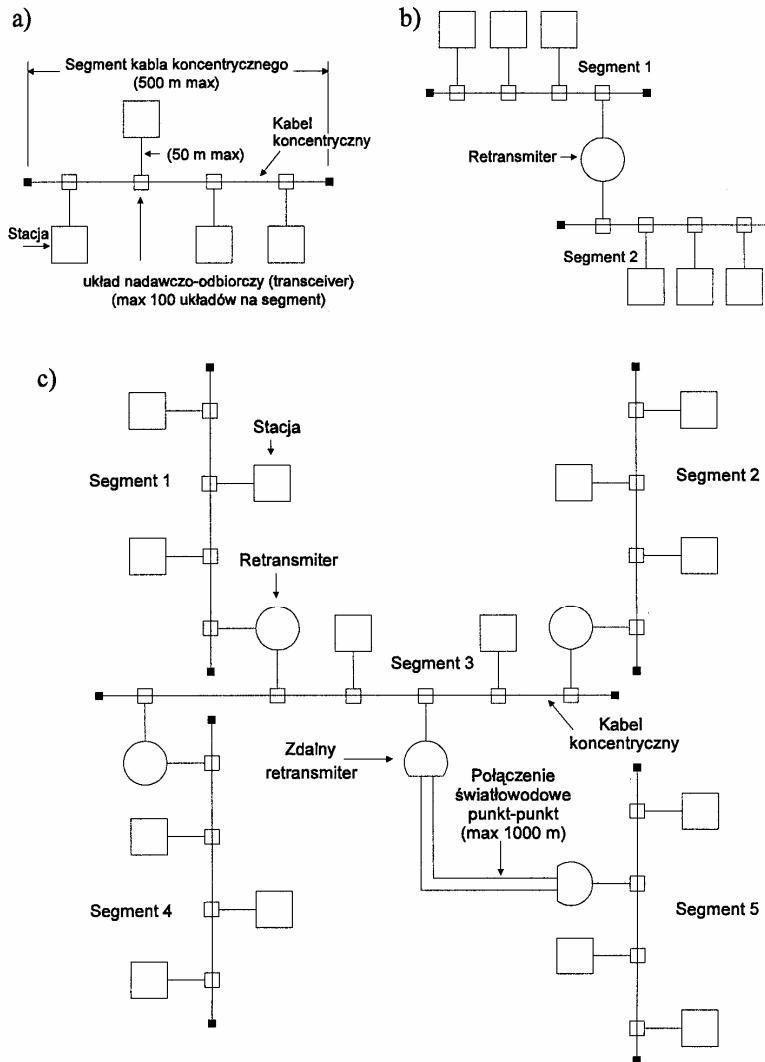
ple Access, por. paragraf 5.2) o funkcję wczesnego wykrywania kolizji (ang. *Collision Detection - CD*), jako metodę dostępu do medium transmisyjnego. Standardowe rozwiązanie sieci Ethernet (typu LAN) zostało przy tym zrealizowane w roku 1981 przez firmy XEROX, DEC i Intel z przeznaczeniem do zastosowań komercyjnych.

#### 4.2.1.1 Podstawowe parametry techniczne

Standard IEEE 802.3 obejmuje szereg wersji sieci LAN umożliwiających transmisję informacji z szybkościami od 1Mb/s do 20Mb/s. W większości rozwiązań znajdujących się na rynku stosowana jest przy tym szybkość 10Mb/s. Transmisja informacji realizowana jest w zasadzie w paśmie podstawowym tj. bez przemiany częstotliwości. Standard IEEE 802.3 dopuszcza jednakże transmisję szerokopasmową (za pośrednictwem mediów szerokopasmowych) i stosowanie przemiany częstotliwości przesyłanych sygnałów. Oba rozwiązania wykorzystują odmienne nadawczo/odbiorcze układy stykowe (ang. MAU - *Medium Attachment Unit*), których istotnym elementem jest układ scalony nadajnika i odbiornika sygnałów. Niektóre rozwiązania MAU umożliwiają dołączenie do nich 8-mu użytkowników (stacji komputerowych). Układ nadawczo-odbiorczy jest w rozwiązaniu standardowym połączony z kartą sieciową użytkownika kablem zakończonym 15-to elementowym złączem (ang. AUI - *Attachment Unit Interface*). Długość tego przyłącza nie może jednakże przekraczać 50 m. Wzajemne usytuowanie układów MAU, DTE i AUI ilustruje rysunek 4.8.



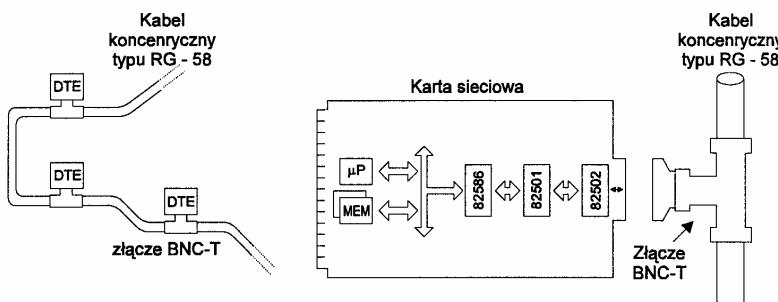
Rys. 4.8. Ilustracja złącza IEEE 802.3



Rys. 4.9. Przykładowe struktury sieci LAN typu IEEE 802.3 łączone za pośrednictwem retransmiterów: a) konfiguracja minimalna (jednosegmentowa), b) konfiguracja dwusegmentowa, c) konfiguracja wielosegmentowa

Struktura sieci LAN jest, zgodnie ze standardem IEEE 802.3, magistralowa, o podstawowej długości 500 m. Poszczególne 500 metrowe segmenty sieci, rea-

lizowane z wykorzystaniem kabla koncentrycznego, mogą być ze sobą łączone za pośrednictwem retransmiterów. Dopuszcza się przy tym stosowanie do 4-ch retransmiterów, co pozwala na tworzenie sieci o maksymalnej długości 2,5 km; (patrz rysunek 4.9). Z kolei maksymalna liczba urządzeń końcowych, które mogą być dołączone do jednego segmentu (liczba kart) wynosi 1024. Gdy zachodzi konieczność tworzenia sieci o większym zasięgu, wówczas należy stosować układy pośredniczące typu most (ang. *bridge*). Na rynku obok rozwiązań standardowych IEEE 802.3, 10BASE5 (10 Mb/s /transmisja w paśmie podstawowym /500 metrowy segment sieci), czy też Ethernet znajdują się rozwiązania tańsze oznaczone np. jako 10BASE2 (gdzie 10 oznacza szybkość transmisji 10Mb/s, BASE transmisję w paśmie podstawowym, a 2 - około 200 metrową długość segmentu), a nazywane Cheapernet. Innym rozwiązaniem jest wersja 10Base-T. W rozwiąaniu Cheapernet stosowany jest cienki kabel koncentryczny RG58 (podczas, gdy w rozwiąaniu standardowym kabel "gruby" RG11). W odróżnieniu od wersji 10BASE5, w 10BASE2 układ nadawczo-odbiorczy umieszczony jest bezpośrednio na karcie sieciowej, a przyłączenie stacji do kabla realizowane jest za pośrednictwem typowego złącza BNC-T (po przecięciu kabla koncentrycznego), co ilustruje rysunek 4.10. Zasięg transmisji i liczby dopuszczalnych układów DTE przyłączonych do jednego kabla są w sieci Cheapernet znacznie mniejsze od przyjętych w IEEE 802.3. Parametry jakościowe są jednak identyczne z osiąganymi w rozwiąaniu standardowym.



Rys. 4.10. Ilustracja realizacji Cheapernet-u

W chwili obecnej coraz większą popularność zyskują rozwiązania sieciowe wykorzystujące skrętki przewodów miedzianych (ekranowanych bądź nieekranowanych). Powszechnie używany akronim 10Base-T opisuje sieć IEEE 802.3 realizującą transmisję z szybkością 10 Mb/s w medium skrętkowym. W rozwiązaniu tym poszczególne stacje dołączone są do wieloportowych hubów, z których każdy pełni rolę magistrali ethernetowej, za pomocą dwóch par skrętek. Długości tych przewodów nie powinny przy tym przekraczać 100 m, przy maksymalnej odległości między skrajnymi użytkownikami (konfiguracja z 4-mi hubami) nie przekraczającej 500 m.

#### 4.2.1.2 Struktura ramki podwarstwy MAC

Struktura ramki definiowanej przez standard IEEE 802.3 pokazana jest na rysunku 4.11. Ramka rozpoczyna się 7 bajtami preambuły, z których każdy jest ciągiem 10101010. Preambuła umożliwia układowi sygnalizacji PLS z warstwy fizycznej (ang. PLS - *Physical Layer Signalling*) osiągnięcie stabilnej synchronizacji bitowej przy odbiorze ramki. Kolejne pole poczyna ramkę właściwą. Pole startu ramki (ang. SFD - *Start Frame Delimiter*) jest ciągiem o postaci 10101011.

Preambuła	Pole startu ramki SFD	Adres stacji docelowej	Adres stacji źródłowej	Długość pola danych	Pole danych podwarstwy LLC	Pole rozszerzenia	Ciąg kontrolny CRC
Liczba bajtów: 7	1	2/6	2/6	2	46 - 1500		4

Rys. 4.11. Struktura ramki w sieci LAN typu IEEE 802.3

Pola adresowe stacji docelowej i źródłowej są 2-u lub 6-cio bajtowe, przy czym ten sam rozmiar pola jest stosowany przez wszystkie stacje danej sieci LAN. Pierwszy bit pola adresu docelowego określa, czy adres ten jest indywidualny, czy grupowy. Podobnie pierwszy bit w polu adresu źródłowego definiuje, czy pole to zawiera adres indywidualny, czy też grupowy, który z kolei może odnosić się do żadnej, jednej, bądź wszystkich stacji LAN.

W adresach 48-bitowych (6 bajtów) drugi bit dokonuje rozróżnienia pomiędzy adresami lokalnymi (L) i globalnymi (uniwersalnymi - U). Adresy globalne administrowane są przez IEEE. Adres grupowy odnosi się zwykle do wielu stacji docelowych i może być:

- adresem obejmującym grupę stacji związaną logicznie zależnościami definiowanymi na wyższym poziomie, bądź
- adresem "rozsiewczym" (rozgłoszeniowym typu broadcast) uwzględniającym wszystkie stacje sieci. W przypadku adresu rozsiewczego wszystkie bity tego pola są jedynkami.

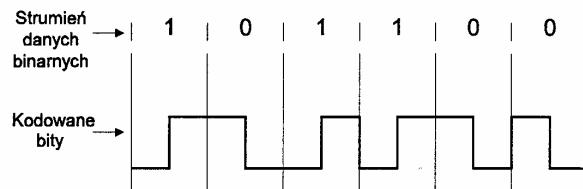
Kolejne dwubajtowe pole określa długość pola danych ramki. Protokół CSMA/CD definiuje minimalną długość ramki równą (bez preambuły i pola startu ramki) 64 bajty (oktety). Jeżeli długość pola danych jest mniejsza niż 46, wówczas pole danych ulega wydłużeniu przez dodanie w polu rozszerzenia (ang. *Pad-padding*) wymaganej liczby bajtów. Zawartość pola danych przygotowywana jest przez podwarstwę kanału logicznego LLC. Długość pola danych specyfikowana przez Ethernet (łącznie z polem pad) może zmieniać się od 46 do 1500 bajtów. W przypadku implementacji IEEE 802.3 z transmisją 10Mb/s w paśmie podstawowym (typ 10BASE5) mamy więc ramki o długościach od 64 do 1518 bajtów. Ostatnie 4-ro bajtowe pole zawiera ciąg kontrolny CRC kodu cyklicznego. Zabezpieczenie CRC nie obejmuje preambuły i ciągu startowego. Przy generacji CRC wykorzystywany jest wielomian CRC-32 o postaci:

$$x^{32} + x^{25} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

#### 4.2.1.3 Zasady transmisji

W przypadku żądania transmisji przez podwarstwę LLC, podwarstwa dostępu MAC konstruuje ramkę poprzez dodanie do pola danych LLC preambuły, ciągu startowego, pól adresowych, pola długości ramki oraz pola kontrolnego CRC.

W protokole CSMA/CD wprowadzenie sygnału do kanału jest poprzedzane nasłuchem stanu kanału (tzw. śledzenie nośnej - *carrier sense*). Dla wersji z 10MHz pasmem podstawowym czas ten nie może być krótszy niż  $9.6\mu s$ . W przypadku, gdy kanał jest wolny, strumień bitów wprowadzanych do medium transmisyjnego jest kodowany w układzie sygnalizacji PLS kodem Manchester. Oznacza to, że szybkość modulacji sygnałów jest dwukrotnie wyższa od szybkości transmisji - patrz rysunek 4.12. Układ nadawczo-odbiorczy umożliwia transmisję i jednoczesny odbiór sygnałów przesyłanych przez medium, a sygnały nadawane są porównywane z odbieranymi (ma miejsce analogowe "monitorowanie" odbieranych sygnałów). W przypadku, gdy nie występuje kolizja ramki przesłanej przez daną stację z innymi ramkami, podwarstwa MAC przekazuje stosowną informację podwarstwie LLC i oczekuje na żądanie przesłania kolejnej ramki. W każdej stacji odbiorczej preambuła ramki wykorzystywana jest do synchronizacji pracy dekodera kodu Manchester. Dekodowane informacje binarne są przesyłane poprzez układ sygnalizacji warstwy fizycznej PLS do podwarstwy dostępu MAC.



Rys. 4.12. Kod Manchester

Podwarstwa MAC usuwa preambułę i ciąg startowy ramki. Bitы odbieranej ramki gromadzone są do chwili, gdy sygnalizowany jest brak sygnału nośnego w kanale. Wówczas dokonywana jest analiza poprawności ramki i jej ewentualne "rozpakowanie". Sprawdzany jest adres docelowy ramki. Jeżeli jest to adres danej stacji, wówczas adresy: źródłowy i docelowy ramki oraz zawartość pola danych LLC przekazywane są do podwarstwy LLC. Do LLC przekazywana jest też informacja o kompletności ramki i poprawności jej długości. Ramki nieprawidłowe są wykrywane przez podwarstwę MAC poprzez kontrolę CRC oraz sprawdzanie poprawności liczby elementów ostatniego oktetu w ramce.

#### 4.2.1.4 Wykrywanie kolizji

*Gdy dwie lub więcej stacji inicjuje transmisje prawie jednocześnie, po stwierdzeniu, że kanał jest wolny, mają miejsce kolizje przesyłanych ramek. Kolizje*

*mogą przy tym wystąpić jedynie na początku transmisji ramek, w tzw. oknie wykrywania kolizji* (ang. *collision window*). W systemie z 10MHz pasmem podstawowym czas trwania okna odpowiada czasowi trwania pojedynczej szczeliny czasowej i wyrażony w bitach wynosi 512b (odpowiada to minimalnej długości ramki). Czas ten jest większy od podwojonego maksymalnego opóźnienia propagacyjnego w kablu. W przypadku, gdy w czasie trwania okna nie została wykryta kolizja stacja może przyjąć, że jest wyłącznym użytkownikiem medium. Długość szczeliny (szerokość okna) musi być przy tym dobrana tak, by stanowiła ona:

- górną granicą czasu pozwalającego na stwierdzenie wyłączności wykorzystywania medium przez stację;
- górną granicę długości części ramki "generowanej przez kolizję", niezbędną do jej wykrycia;
- kwantem czasu potrzebnym na rozpoczęcie retransmisji ramki.

Ażeby spełnić 3 powyższe wymagania, czas trwania szczeliny musi być większy od sumy podwojonego maksymalnego opóźnienia propagacyjnego w kanale fizycznym oraz maksymalnego czasu zakłócania (ang. *maximum jam time*). Wielkości te są zdeterminowane właściwościami medium transmisyjnego (maksymalna długość kabla, szybkość propagacji) oraz szybkością pracy układów wejściowych.

Kolizja ramek wykrywana jest przez elementy podwarstwy MAC. *Wykryciu kolizji towarzyszy przerwanie transmisji ramki i generacja sygnału zakłócającego, zmuszającego wszystkie stacje do zaprzestania realizowanych przez nie transmisji.* Sygnał zakłócający jest w sieci z transmisją 10Mb/s ciągiem 32 bitowym. *Kolejna transmisja ramki realizowana jest zgodnie z procedurą nazywaną algorytmem z binarnym-wykładniczym rozszerzaniem czasu (okna) rywalizacji* (ang. *binary-exponential back-off*). Algorytm stosowany w IEEE 802.3 realizuje przy pierwszej próbie dostępu do kanału procedurę CSMA z wymuszaniem transmisji z prawdopodobieństwem 1. Oznacza to, że po stwierdzeniu braku zajętości kanalu następuje natychmiastowa transmisja ramki. W przypadku kolizji ramki przedział, w którym może być dokonana jej retransmisja (okno rywalizacji - randomizacji) jest rozszerzany do 2-ch szczelin, przy czym wybór każdej z nich jest losowy z prawdopodobieństwem 0.5. Po kolejnej kolizji przedział retransmisji powiększa się do 4-ch szczelin, z prawdopodobieństwem ich wyboru równym 0.25. Rozszerzanie przedziału randomizacji trwa do 10 kolejnych kolizji, gdy przedział ten osiąga 1024 szczeliny. Szerokość tego przedziału ulega wówczas „zamrożeniu”, a kolejne kolizje, do 15-tej włącznie, nie powodują zmiany tej szerokości. Kolizja 16-ta powoduje wstrzymanie procesu retransmisji i sygnalizację niesprawności.

#### 4.2.1.5 Ocena jakości pracy sieci LAN z protokołem CSMA/CD

Przedstawimy obecnie przybliżoną analizę jakości standardu IEEE 802.3, zakładając stałą i znaczną wartość obciążenia sieci. Oznacza to, że w przypadku dużej populacji stacji średnia liczba stacji mających ramki do przesłania jest

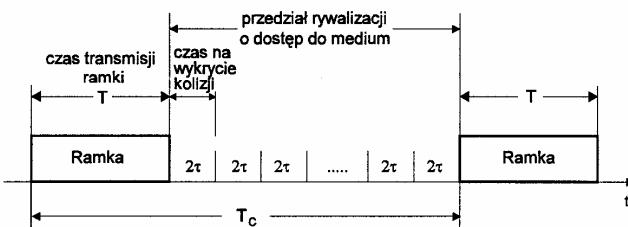
dużej niż 1. Dokładna analiza systemu CSMA/CD z binarnym-wykładowicznym rozszerzeniem czasu retransmisji jest bardzo skomplikowana. Badania symulacyjne wykazały jednak, że przyjęcie modelu z geometrycznym rozkładem czasu rywalizacji o dostęp do medium dobrze przybliża pracę stacji w sieci rzeczywistej.

Jakość protokołów klasy CSMA, w tym i CSMA/CD, zależy w sposób bardzo silny od parametru  $a = \tau / T$ , gdzie zgodnie z oznaczeniami przyjętymi przy analizie protokołów warstwy łączącej danych w sieciach rozległych czas transmisji ramki  $T$  wynosi  $T=F/c$ , a  $\tau$  jest maksymalnym opóźnieniem propagacyjnym w sieci.

Przedmiotem rozważań będzie wykorzystanie całkowitego  $U_c$  kanału (maksymalny przepływ ramek bądź przepustowość systemu) definiowane jako iloraz

$$U_c = \frac{T}{T_c}$$

gdzie  $T_c$  jest zgodnie z ilustracją podaną na rysunku 4.13 czasem trwania cyklu transmisyjnego.



Rys. 4.13. Ilustracja czasu trwania cyklu transmisyjnego  $T_c$

Wybierając dwie skrajne stacje sieci IEEE 802.3 należy wyznaczyć maksymalne opóźnienie  $\tau$ . Podwojona wartość tego opóźnienia daje nam przybliżoną długość czasu trwania szczeliny, czyli okna wykrywania kolizji; oczywiście w gotowych produktach dostępnych na rynku szerokość okna jest stała i niezależna od konfiguracji sieci.

Przy dużym obciążeniu sieci w pracy medium wyróżniamy występujące kolejno udane transmisje ramek (o czasie trwania  $T$ ) i okresy rywalizacji o średniej długości  $J$  szczelin (2 $\tau J$  sekund). Tym samym

$$T_c = T + 2\tau J = T(1 + 2aJ).$$

Wartość  $J$  zależy oczywiście od strategii retransmisji. Przyjmując geometryczny model rozkładu czasu rywalizacji o dostęp do medium  $J$  możemy wyrazić jako

$$J = \sum_{k=1}^{\infty} kv(1-v)^{k-1} = \frac{1}{v},$$

gdzie  $v$  jest prawdopodobieństwem udanej transmisji ramki. Zakładając, że liczba stacji jest duża ( $N \gg 1$ ) prawdopodobieństwo to możemy opisać wzorem

$$v = Np(1-p)^{N-1},$$

w którym  $p$  jest prawdopodobieństwem rozpoczęcia transmisji w wybranej szczeblinie przez określoną stację. Maksymalne wykorzystanie kanału  $U_c$  otrzymamy, gdy  $v = v_{\max}$ , a tym samym czas trwania przedziału rywalizacji ( $2\tau J$ ) jest minimalny. Maksymalną wartość  $v$  otrzymujemy dla  $p = 1/N$ .

Zatem

$$v_{\max} = \left(1 - \frac{1}{N}\right)^{N-1} \xrightarrow[N \rightarrow \infty]{} e^{-1}$$

Ostatecznie dla  $N \rightarrow \infty$  mamy

$$T_c = T(1 + 2ae)$$

oraz

$$U_c = \frac{1}{1 + a(1 + 2ae)}.$$

Wprowadzając dodatkowo takie parametry jak:

L - długość kabla w sieci IEEE 802.3

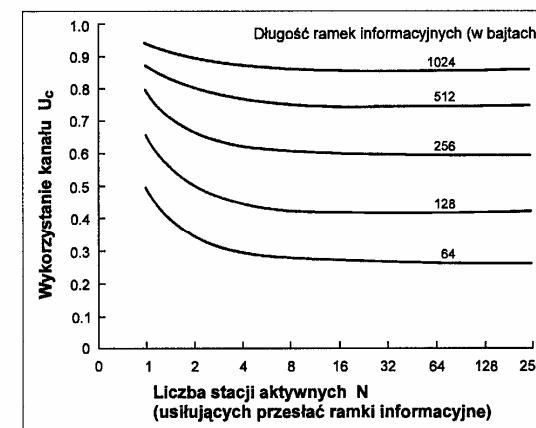
C - szybkość propagacji w kablu

F - długość ramki w bitach

c - szybkość transmisji w b/s

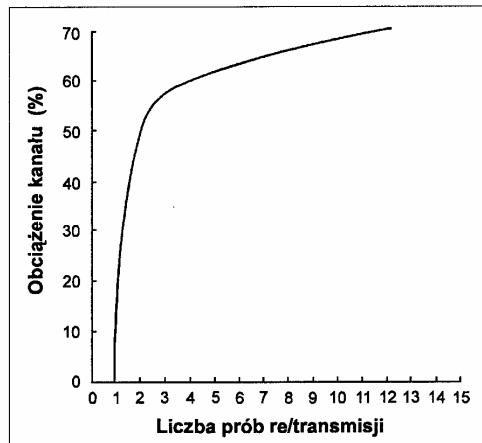
otrzymujemy

$$U_c = \frac{1}{1 + 2cLe / CF}.$$

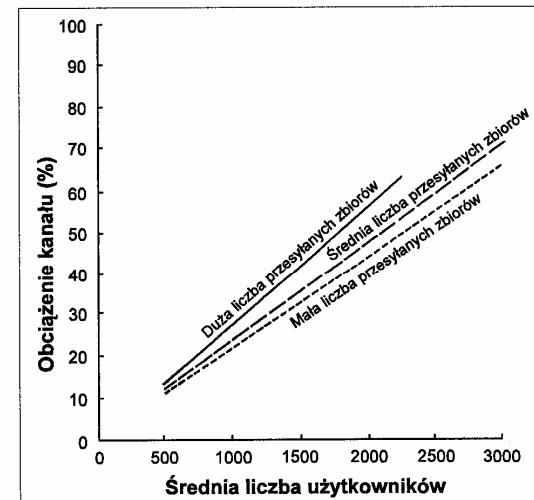


Rys. 4.14. Zmiany wykorzystania medium  $U_c$  przy zmianie liczby stacji aktywnych ( $N$ ) dla różnych długości  $F$  ramek informacyjnych (dla standardu IEEE 802.3 z  $c=10$  Mb/s i długością szczelin rywalizacji 512b)

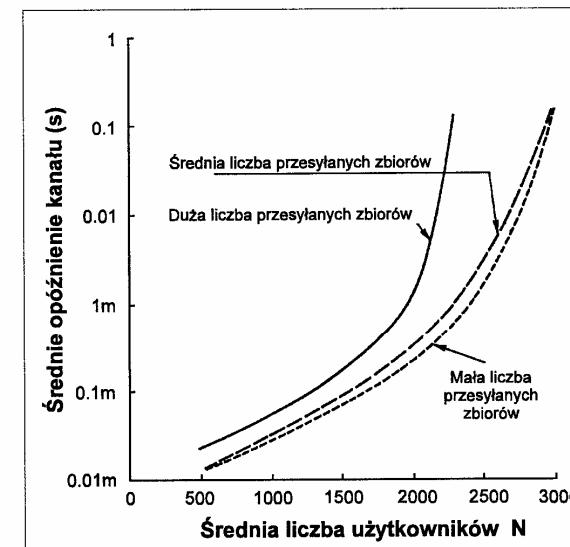
*Sieć IEEE 802.3 pracująca z nominalną szybkością transmisji 10Mb/s może przenosić dane z rzeczywistą szybkością do 9Mb/s. Jednakże wartość ta ulega istotnemu ograniczeniu, gdy obciążenie kanału transmisyjnego (ruch oferowany przez stacje końcowe) rośnie. Przyczyną tego są liczne kolizje i konieczność wielokrotnych prób re/transmisji ramek.* Rysunek 4.15 prezentuje zależność pomiędzy liczbą prób transmisji a oferowanym obciążeniem w typowym 10Mb/s systemie Ethernet. Gwałtowny wzrost liczby prób transmisji ramki następuje po przekroczeniu 60-cio procentowego progu obciążenia kanału (jego wypełnienia czasowego). Przy tych warunkach opóźnienie w dostępie do kanału rośnie gwałtownie. Sprawia to, że standard IEEE 802.3 nie może być stosowany do obsługi zgłoszeń w czasie rzeczywistym. System z protokołem CSMA/CD nie gwarantuje bowiem ograniczonego opóźnienia w dostępie. W przypadku, gdy czas dostępu jest parametrem krytycznym, zdecydowanie lepsze są systemy z przepływnikiem lub przekazywaniem znaczników (tokenów) i wykorzystującą priorytety. Pomimo wspomnianego powyżej ograniczenia rozwiązań IEEE 802.3 standard ten jest najczęściej stosowany. Największą popularność zyskał on w zastosowaniu do automatyzacji biur i w środowiskach uniwersyteckich. Rysunek 4.16 przedstawia przykładowe procentowe zmiany obciążenia dużej uniwersyteckiej sieci Ethernet przy zmianie średniej liczby stacji końcowych dla różnych rodzajów przesyłanych danych. Kolejny rysunek 4.17 prezentuje zmiany opóźnienia w dostępie do tej samej sieci Ethernet. Należy zwrócić uwagę na fakt, że szybkość przekazu danych bywa częściej ograniczana możliwościami lokalnego procesora do realizacji funkcji warstw 2-7 w modelu ISO/OSI niż możliwościami transmisyjnymi sieci bądź elementów układu DTE (karta sieciowa) do przenoszenia danych z/do pamięci lokalnej.



Rys. 4.15. Zależność pomiędzy obciążeniem typowej sieci Ethernet (10 Mb/s), a liczbą prób re/transmisji ramek



Rys. 4.16. Zmiany obciążenia przykładowej sieci Ethernet przy zmianie średniej liczby użytkowników



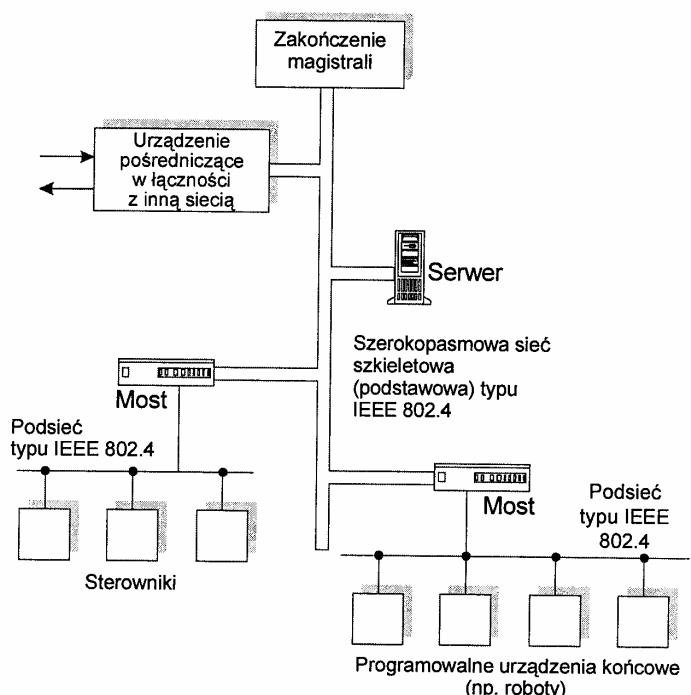
Rys. 4.17. Zmiany opóźnienia w dostępie do przykładowej sieci Ethernet przy zmianach średniej liczby użytkowników

## 4.2.2 Protokół tokenowy dla sieci magistralowej - Standard IEEE 802.4

**Standard IEEE 802.4** (ang. *token bus LAN*) został opracowany głównie z myślą o zastosowaniu do automatyzacji przedsiębiorstw. Podobnie jak IEEE 802.3, standard IEEE 802.4 specyfikuje funkcje i zasady pracy warstwy fizycznej oraz części warstwy łączącej danych, czyli podwarstwy dostępu do medium MAC.

### 4.2.2.1 Podstawowe parametry

W przypadku zastosowań przemysłowych standard IEEE 802.4 stanowi zwykle część warstwowej architektury (tzw. profil) **Protokołu Automatyzacji Przedsiębiorstwa** (ang. MAP - Manufacturing Automation Protocol). Warstwa fizyczna może współpracować zarówno z tzw. szerokopasmowym  $75\Omega$  kablem koncentrycznym (stosowanym w instalacjach TV kablowej), w którym wydziela się częstotliwościowo od kilku do kilkunastu podkanalów, z których każdy umożliwia transmisję z szybkością do  $10\text{Mb/s}$  jak też z pojedynczym kanałem z wykorzystaniem modulacji pasmowej.



Rys. 4.18. Przykład sieci MAP

W przypadku systemów MAP protokoły IEEE 802.4 stosowane są zarówno w sieci podstawowej (ang. *backbone network*), łączącej odległe jednostki organizacyjne przedsiębiorstwa, jak też w podsieciach lokalnych przyłączonych do sieci podstawowej za pośrednictwem mostów, zgodnie z ilustracją pokazaną na rysunku 4.18. Podsieci operujące zgodnie ze standardem IEEE 802.4 obejmują małe obszary i wykorzystują do transmisji pojedyncze kanały z modulacją pasmową, podczas gdy sieć podstawowa wykorzystuje zwykle kanały szerokopasmowe. W obu przypadkach stosowane są modulacje FSK. W rozwiązaniu pasmowym-jednokanałowym pojedynczy segment sieci o długości 1 km umożliwia dołączenie do 30 stacji końcowych. Zasięg podsieci można rozszerzyć stosując układy retransmisyjne. W przypadku medium szerokopasmowego, stosowanego w sieci podstawowej, odległość stacji od kabla może sięgać do 30 m.

**Zasada pracy sieci magistralowej (szynowej) ze znacznikami (tokenami) jest rozwinięciem techniki przepływu z przekazywaniem przepustki** (ang. hub polling). Stacje aktywne dołączone do medium tworzą pętlę logiczną. Kolejność stacji w tej pętli może być przy tym odmienna od kolejności fizycznego dołączenia stacji do magistrali. Każda stacja znajdująca się w pętli zna adresy (identyfikatory) stacji poprzedzającej ją w pętli (ang. predecessor) oraz stacji kolejnej w pętli (ang. successor). Stacja, która odbiera adresowany do niej token (przepustkę, znacznik), nabywa prawo dostępu do medium. Tym samym przejmuje ona sterowanie siecią i może przesyłać przygotowane ramki informacyjne. Dostęp do sieci jest więc regulowany i bezkolizyjny, gdyż tylko posiadacz przepustki może przesyłać informacje. Po zakończeniu transmisji, stacja przekazuje token do stacji kolejnej w pętli logicznej. Tym samym zagwarantowany jest cykliczny obieg tokena i sprawiedliwy algorytm dostępu do medium.

Protokół tokenowy dla sieci magistralowej jest bardzo złożony. Obejmuje on szereg procedur związanych z utrzymaniem pętli logicznej, jej inicjowaniem, przywracaniem prawidłowej pracy stacji w przypadku straty tokena, dodawaniem nowych stacji do pętli logicznej bądź też ich usuwaniem z pętli. Przy prawidłowej pracy sieci możemy wyróżnić dwie występujące naprzemian fazy, tj. przekazu danych i przesyłania tokena. Zakładając, że znane są długości tych faz, jesteśmy w stanie określić opóźnienie w dostępie stacji do medium. Dodatkowo, zastosowanie priorytetów wewnętrznych w każdej ze stacji zapobiega opóźnianiu transmisji ramek o wysokim priorytecie obsługi.

### 4.2.2.2 Format ramki w sieci magistralowej z tokenami

Jeden standardowy format, pokazany na rysunku 4.19, używany jest dla ramek informacyjnych, przepustki-tokena oraz ramek utrzymywanych MAC (ang. ring maintenance). Ramka właściwa poprzedzana jest, podobnie jak w standardzie CSMA/CD IEEE 802.3, ciągiem preambuły oraz jednobajtowym ciągiem początku ramki. Preambuła pozwala na osiągnięcie synchronizacji przy odbiorze ramki.



Rys. 4.19. Format ramki w standardzie IEEE 802.4

Kolejne pole (1 oktet) określa typ ramki, która może być:

- ramką informacyjną
- ramką sterująco-kontrolną
- ramką utrzymywianą podwarstwy MAC.

W odróżnieniu do ramek utrzymywanych podwarstwy MAC wyróżnia się:

- a) przepustkę (ang. *token*)
- b) żądanie tokena (ang. *claim token*)
- c) ustalanie następcy w pętli (ang. *set successor*)
- d) ubieganie się o dołączenie (ang. *solicit successor*)
- e) rozwiązywanie rywalizacji (ang. *resolve contention*)
- f) kto następny (ang. *who follows*).

Ramki danych (informacyjne) zawierają bity określające priorytet ramki (do 8 poziomów priorytetu). Adresy źródłowy i docelowy mogą być dwu lub sześciobajtowe. Adresy grupowe i rozsiewcze są definiowane tak jak w standardzie CSMA/CD IEEE 802.3. Pole danych ramki może zawierać informację przeslaną z podwarstwy LLC, informację kontrolną podwarstwy MAC, pozwalającą na zarządzanie dostępem do medium (ang. *medium access control management*), względnie właściwy parametr związany z rodzajem ramki sterującej. Nie ma przy tym ograniczeń minimalnej długości pola danych. Ograniczeniem podlega natomiast maksymalna długość ramki; liczba oktetów (bajtów) pomiędzy znakami początku i końca nie może przekraczać 8191.

Kolejne pole jest ciągiem kontrolnym CRC kodu cyklicznego generowanego przez wielomian identyczny jak w IEEE 802.3 (CRC-32). Ciąg ten zabezpiecza pola ramki znajdujące się pomiędzy ciągiem początku i końca ramki.

Jeden z bitów ciągu końca ramki wykorzystywany jest przy tym jako wskaźnik kontynuacji lub zakończenia transmisji ramek przez stację.

Inny bit może być wykorzystywany przez stację retransmitującą ramkę do wskazania, że został wykryty błąd.

W przypadku, gdy bezpośrednio po ciągu początku ramki przesłany zostaje ciąg jej końca, oznacza to przerwanie transmisji.

Ramka informacyjna ma dla danej implementacji sieci magistralowej ścisłe określoną liczbę bajtów organizacyjno-sterujących (ustaloną długość nagłówka). Różnice implementacyjne dotyczą:

- a) Preambuły, która może zmieniać się przy różnych szybkościach transmisji w magistrali.  
Minimalny czas trwania preambuły wynosi  $2\mu s$  i składa się z całkowitej liczby oktetów. Oznacza to 1 oktet dla magistrali z 1Mb/s i 3 oktetów dla magistrali 10Mb/s.
- b) Długości pól adresów: źródłowego i docelowego, które mogą być 16-bitowe lub 48-bitowe, w zależności od przyjętej opcji.

#### 4.2.2.3 Zasady transmisji

Stacja aktywna jest w każdej chwili gotowa do odbioru ramki, z wyjątkiem okresu, gdy jest ona w posiadaniu tokena. Stacja chcącą przesyłać ramkę musi natomiast czekać na odbiór tokena. Po jego przyjęciu stacja może przesyłać dowolną liczbę ramek, ograniczoną jednakże przez przyjęty system priorytetów i maksymalny czas posiadania przez stację tokena.

System priorytetów narzuca wymóg pomiaru przez stacje czasu obiegu tokena wokół pętli logicznej. *Wiadomości przesypane przez stacje podzielone są na klasy dostępu: 6, 4, 2, 0 i ramki utrzymywane pętli, a pewien nominalny czas cyrkulacji (obiegu) tokena jest definiowany dla każdej klasy wiadomości, z wyjątkiem klasy 6, najwyższej, gdyż wiadomości te muszą być transmitowane bez względu na czas obiegu tokena.* Dane o niższych priorytetach są przesyłane jedynie wtedy, gdy czas obiegu tokena mierzony przez stację dla ostatniego cyklu jest mniejszy od progowego czasu przypisanego wiadomościom o danym priorytecie.

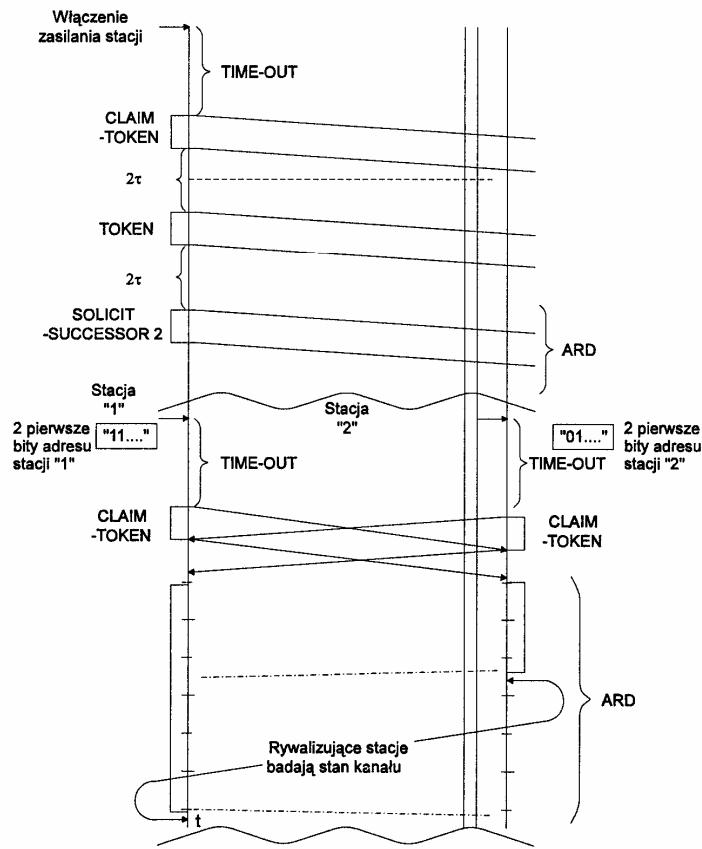
Przesyłane wiadomości są odbierane przez wszystkie stacje, lecz tylko jedna docelowa (lub grupa stacji) odczytuje dane zawarte w ramce. Po zakończeniu transmisji ramek token jest przekazywany stacji kolejnej w pętli logicznej.

W odróżnieniu od skoncentrowanych algorytmów przepływu (ang. *polling*), w standardzie IEEE 802.4 realizowane jest zdecentralizowane sterowanie dostępem do medium. Nie ma zatem centralnej stacji monitorującej pracę sieci i generującej tokeny.

**Proces inicjowania pętli logicznej** ma miejsce, gdy w sieci nie istnieje pętla, przy czym może to się wiązać z rozpoczęciem pracy przez stacje sieci, lub też z utratą tokena, spowodowaną uszkodzeniem stacji.

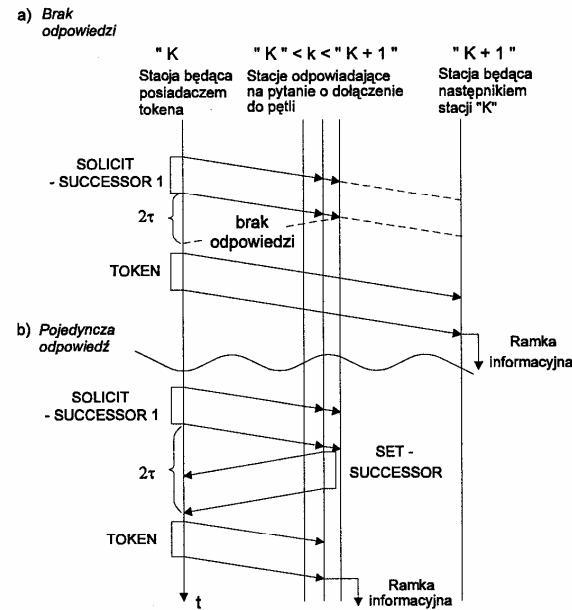
Po upływie czasu badania kanału (time-out), stacja nie wykrywająca aktywności w magistrali wysyła ramkę żądania tokena CLAIM-TOKEN (C-T). Brak innych ramek C-T sprawia, że stacja staje się posiadaczem tokena. W celu powiększenia pętli logicznej stacja wysyła periodycznie ramki SOLICIT-SUCCESSOR z zaproszeniem dołączenia do pętli. W przypadku pojawiienia się kilku ramek

C-T rywalizacja stacji zgłoszających swój akces do pętli logicznej rozstrzygana jest w sposób zbliżony do opisanego w CSMA/CD. Każda konkurująca do przejęcia tokena stacja wysyła ramkę C-T rozszerzoną o 0, 2, 4 lub 6 szczelin czasowych (będących w przybliżeniu podwojonym czasem  $\tau$ ). Długość czasu transmisji wynika przy tym z wartości dwóch pierwszych bitów adresu stacji. Po zakończeniu swojej transmisji stacja bada stan kanału. Jeżeli stwierdza zajętość kanału to rezygnuje z ubiegania się o token, w przeciwnym przypadku ponawia próbę wydłużając czas transmisji o 0, 2, 4 lub 6 szczelin, zgodnie z wartościami dwóch kolejnych bitów adresu (najczęściej brany jest pod uwagę 6-cio bajtowy adres fizyczny stacji). Proces rywalizacji ARD (Algorytm Rywalizacji o Dołączenie do pętli logicznej) ilustruje rysunek 4.20. Zwycięska stacja jest pierwszą stacją w tworzonej pętli logicznej.



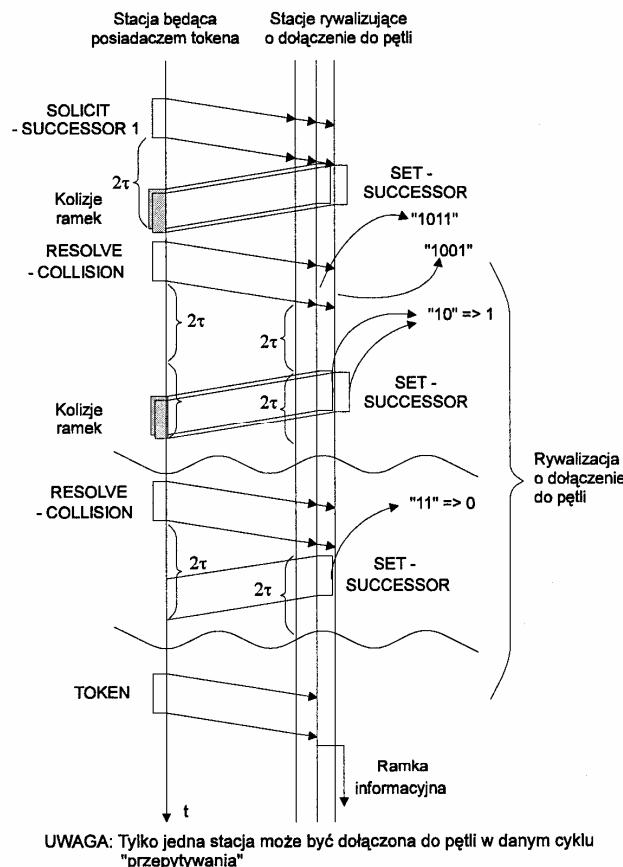
Rys. 4.20. Inicjowanie pętli logicznej

Proces rozszerzania liczby stacji w pętli logicznej musi być kontynuowany, zapewniając pozostałym stacjom możliwość ich dołączenia do pętli.

Rys. 4.21. Ilustracja działania sieci po wysłaniu ramki SOLICIT-SUCCESSOR:  
a) brak odpowiedzi, b) pojedyncza odpowiedź

Za proces dodawania stacji do pętli odpowiedzialne są stacje aktywne znajdujące się w pętli. Każda z tych stacji okresowo sprawdza, czy istnieją stacje nie należące do pętli logicznej. Odbiera się to w okresie, gdy stacja jest w posiadaniu tokena i dysponuje rezerwą czasu pozwalającą na przesłanie ramek zarządzających. W tym celu stacja przesyła ramkę SOLICIT-SUCCESSOR (ubieganie się o dołączenie) zapraszającą nowe stacje do dołączenia się do pętli. Możliwe są różne scenariusze związane z brakiem odpowiedzi, jedną lub wieloma odpowiedziami. Każdorazowo stacja wysyłająca ramkę SOLICIT-SUCCESSOR otwiera tzw. okno odpowiedzi, oczekując przez czas  $2\tau$  na ewentualny odbiór ramki SET-SUCCESSOR z adresem nowej stacji. Różne warianty działania stacji po wysłaniu SOLICIT-SUCCESSOR ilustruje rysunek 4.21. Przy braku odpowiedzi stacja przekazuje token stacji kolejnej w pętli. W przypadku odbioru pojedynczej ramki SET-SUCCESSOR, token zostaje przekazany nowej stacji. Natomiast w przypadku kilku odpowiedzi, stacja będąca posiadaczem tokena inicjuje procedurę rozwiązywania konfliktu przesyłając ramkę RESOLVE-COLLISION. Po jej odbiorze stacje ubiegające się o dostęp dzielą o czasu pracy kanału na szczeliny

(kwanty czasu) o długości  $2\tau$  i wybierają jedną z nich zgodnie z wartościami kolejnych par bitów ich adresów MAC (patrz rysunek 4.22) poczynając od bitów najbardziej znaczących. Na podstawie odpowiedzi SET-SUCCESSOR stacja inicjująca procedurę dołączania wybiera tylko jedną ze stacji, o numerze właściwym z punktu widzenia organizacji pętli, czyniąc tę stację, stacją kolejną w pętli i przekazując jej token.

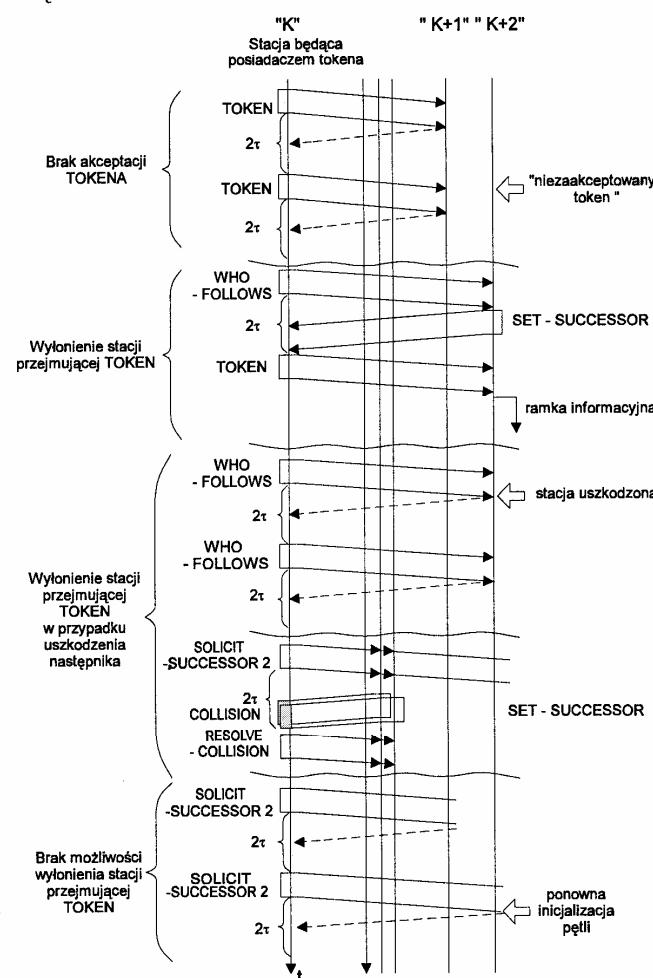


Rys. 4.22. Proces dołączania nowych stacji do pętli w przypadku wielu stacji ubiegających się o dołączenie

**Opuszczenie pętli logicznej przez stację** jest możliwe dopiero po przejęciu przez tę stację tokena. W celu realizacji usunięcia z pętli stacja wysyła ramkę SET-SUCCESSOR, która łączy w pętli logicznej stację poprzedzającą, opuszczającą pętlę, ze stacją kolejną, która staje się jednocześnie posiadaczem tokena.

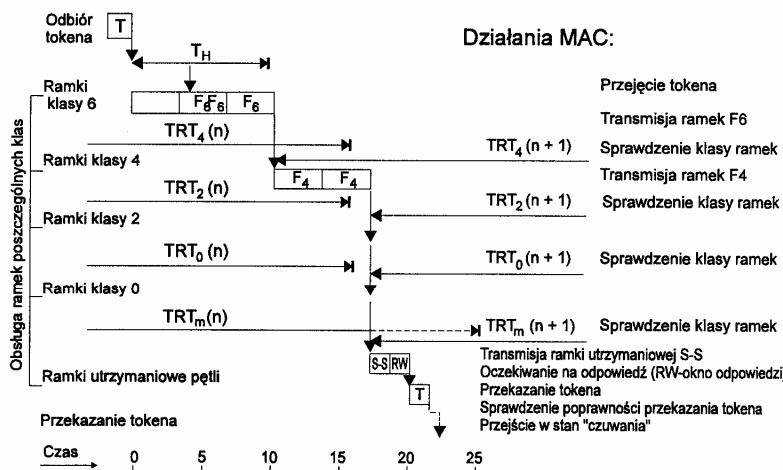
Niezależnie od opisanych powyżej procedur **protokół warstwy MAC nadzoruje prawidłową pracę pętli** reagując na:

- 1) pojawiение się kilku ramek typu token,
- 2) brak akceptacji tokena,
- 3) uszkodzenie stacji,
- 4) brak stacji odbiorczej,
- 5) stratę tokena.



Rys. 4.23. Przykładowe działanie podejmowane przez stacje w przypadku nieprawidłowej pracy pętli

Przykładowe działania podejmowane przez stację ilustruje rysunek 4.23. W przypadku pojawienia się kilku tokenów, stacje rezygnują z transmisji. Prowadzi to zwykle do ponownego inicjowania pętli. Każda stacja, po przesłaniu tokena, musi badać stan kanału, by stwierdzić, czy adresat tokena podjął transmisję. W przypadku braku aktywności w kanale token zostaje przesłany po raz drugi. Ponowny brak aktywności adresata tokena powoduje wysłanie ramki WHO-FOLLOWS, pozwalającej na identyfikację stacji następnej. Adres zawarty w ramce odpowiedzi SET-SUCCESSOR umożliwia zamknięcie pętli logicznej z ominięciem stacji wyłączonej lub uszkodzonej. Brak odpowiedzi typu SET-SUCCESSOR powoduje, że posiadacz tokena przerwą transmisję i rozpoczyna procedurę inicjowania pętli.



Rys. 4.24. Diagram ilustrujący pracę wybranej stacji, łącznie z przesaniem ramki utrzymywanej SOLICIT - SUCCESSOR

W przypadku, gdy wszystkie stacje aktywne znajdują się poza pętlą, możemy mówić o normalnej pracy sieci. Na rysunkach 4.24 i 4.25 przedstawiono diagramy ilustrujące pracę wybranej stacji od chwili odbioru tokena, do momentu przekazania go stacji kolejnej. Przyjęto przy tym następujące oznaczenia:

- osziostra reprezentuje upływający czas,
- przesypane ramki przedstawione są w postaci bloków prostokątnych, gdzie:

$T$  - token,  
 $F_i$  - ramka informacyjna z klasą dostępu  $i$  (priorytetem) jako indeksem dolnym ( $F_i$ )),  
 $S$  - SOLICIT-SUCCESSOR (dołączenie stacji następnej),  
 $RW$  - okno odpowiedzi,

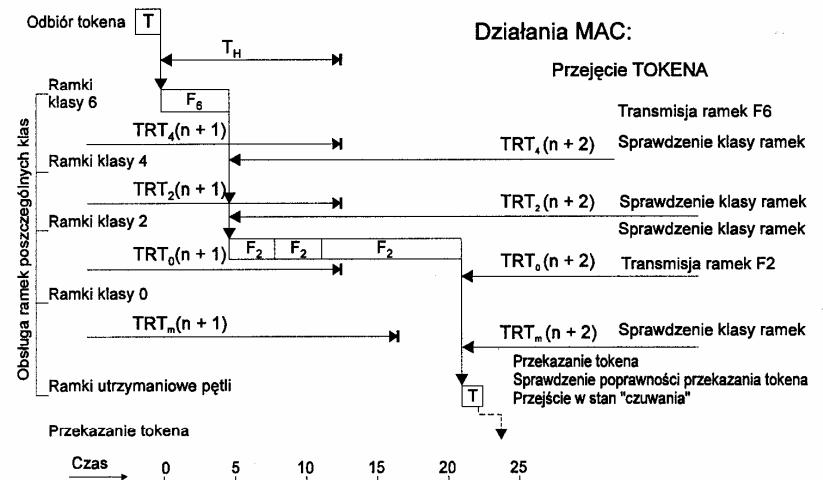
#### 4.2.2 Protokół tokenowy dla sieci magistralowej - Standard IEEE 802.4

- czas odliczane przez liczniki stacji przedstawione są jako linie poziome,

- oznaczenia liczników są następujące:

$T_H$  - czas obsługi zgłoszeń o najwyższy priorytetie,  
 $TRT_i(n)$  - czas obiegu tokena dla wiadomości z klasą dostępu „ $i$ ” w  $n$ -tym cyklu transmisyjnym; klasa dostępu „ $m$ ” dotyczy ramek utrzymywanych pętli.

W momencie odbioru tokena uruchomiony zostaje licznik czasu posiadania tokena i przejście do stanu obsługi ramek zgromadzonych w buforach stacji. Proces obsługi rozpoczyna się od wysłania informacji o najwyższym priorytecie (ramki  $F_6$ ). Długości ramek jak i adresy ich przeznaczenia mogą być różne. Jeżeli w trakcie obsługi 3-ciejs ramki klasy 6 upływa czas  $T_H$  przeznaczony na obsługę tej klasy, kolejne ramki  $F_6$  nie mogą być przesypane. Stacja przechodzi do obsługi zgłoszeń klasy 4 ( $F_4$ ) z odpowiadającym tej klasie czasem obiegu tokena  $TRT_4(n)$ .



Rys. 4.25. Diagram ilustrujący pracę wybranej stacji

Po upływie czasu obsługi ramek  $F_4$  stacja zawiesza obsługę zgłoszeń klasy 2 i 0, gdyż wyznaczony dla nich czas obiegu tokena upłynął. Pozostały czas, w którym stacja jest posiadaczem tokena, przeznaczony jest na obsługę pętli. Na rysunku 4.24 czas ten jest wykorzystany na przesłanie zapytania SOLICIT-SUCCESSOR (S-S) o chęć dołączenia nowej stacji do pętli. W przypadku, gdy wszystkie stacje zostały już dołączone do pętli, w oknie odpowiedzi (Response window) nie

pojawi się żadne zgłoszenie typu SET-SUCCESSOR. Tym samym stacja kończy okres transmisji i po wysłaniu tokena przechodzi w stan spoczynku.

Kolejny rysunek 4.25 przedstawia nieco odmienną sytuację, w szczególności:

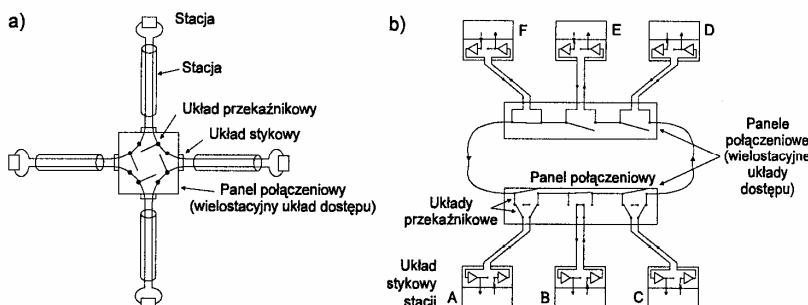
- wiadomości o najwyższym priorytecie nie wykorzystują całej puli czasu  $T_H$ ,
- czas  $TRT_4(n+1)$  upływa zanim wiadomości tej klasy uzyskują dostęp do medium, tym samym nie są one obsługiwane,
- $TRT_4(n+1)$  pozwala na przesłanie 3-ch ramek  $F_2$ ,
- upływ czasu  $TRT_0(n+1)$  podczas transmisji ramki  $F_2$  nie pozwala na obsługę ramek klasy 0,
- wyznaczony dla ramek utrzymywanych czas obiegu tokena  $TRT_m(n+1)$  kończy się w trakcie przesyłania ramki  $F_2$ . Tym samym stacja nie może wysłać zapytania SOLICIT-SUCCESSOR do ewentualnych stacji aktywnych znajdujących się poza pętlą.

### 4.2.3 Protokół tokenowy dla sieci pętlowej - Standard IEEE 802.5

Standard IEEE 802.5 definiuje metodę dostępu do medium oraz specyfikuje funkcjonowanie warstwy fizycznej w sieci pętlowej. Rozwiązanie to oparte jest na koncepcji IBM-owskiej pętlowej sieci LAN.

#### 4.2.3.1 Podstawowe dane techniczne

Cechą charakterystyczną sieci pętlowych jest to, że pętla nie jest w rzeczywistości medium propagacyjnym, lecz zespołem odcinków łącz typu punkt-punkt tworzących pierścień.

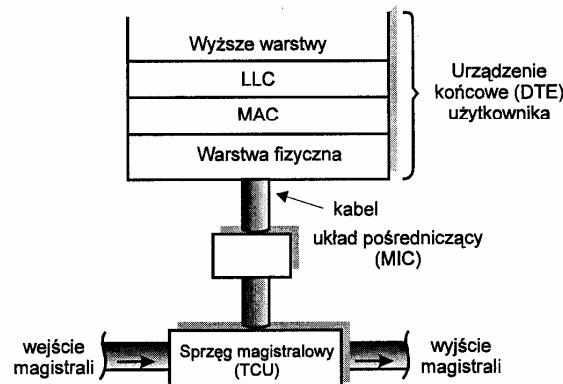


Rys. 4.26. Przykładowe konfiguracje sieci pętlowej: a) z pojedynczym panelem połączeniowym, b) z dwoma panelem połączeniowymi

Przy realizacji pętli fizycznej można przy tym wykorzystać skrętki przewodów, kable koncentryczne bądź światłowody. W większości sieci pętlowych, w tym

w sieciach IBM, poszczególne stacje dołączone są do sieci za pośrednictwem wielostacyjnych układów dostępu (ang. MAU - Multistation Access Unit) zlokalizowanych najczęściej, ze względów diagnostycznych, w jednym miejscu, co nadaje sieci wygląd gwiazdy, patrz rys. 4.26. W sieci IBM typowa szybkość transmisji wynosi 4Mb/s. Standard IEEE 802.5 dopuszcza też szybkości 1Mb/s i 16 Mb/s. Stacje użytkowników mogą być oddalone od układu dostępu MAU do 100 m w przypadku wykorzystania skrętek przewodów, lub 200 m w przypadku skrętek izolowanych bądź światłowodów.

IEEE 802.5 specyfikuje standardowy układ pośredniczący dostępu do medium (ang. MIC - Medium Interface Connector) przyłączający stację (jej adapter sieciowy) do układu sprzęgu magistralowego (ang. TCU - Trunk Coupling Unit) zgodnie z ilustracją (rysunek 4.27). Pokazane na rysunku 4.26 elementy przekaźnikowe, pozwalające na usuwanie z pętli (przez zwieranie) stacji uszkodzonych lub dołączanie stacji sprawnych, stanowią elementy układów TCU. Sygnały binarne, przed wprowadzeniem do kanału, kodowane są różnicowym kodem Manchester.



Rys. 4.27. Ilustracja dołączenia stacji do pętli (magistrali)

W celu wydłużenia magistrali (pętli) można stosować regeneratory. Każdy regenerator traktowany jest przy tym jako jedna spośród maksymalnie 250 stacji. Użycie mostów pozwala z kolei na połączenie do 7-mu pętli.

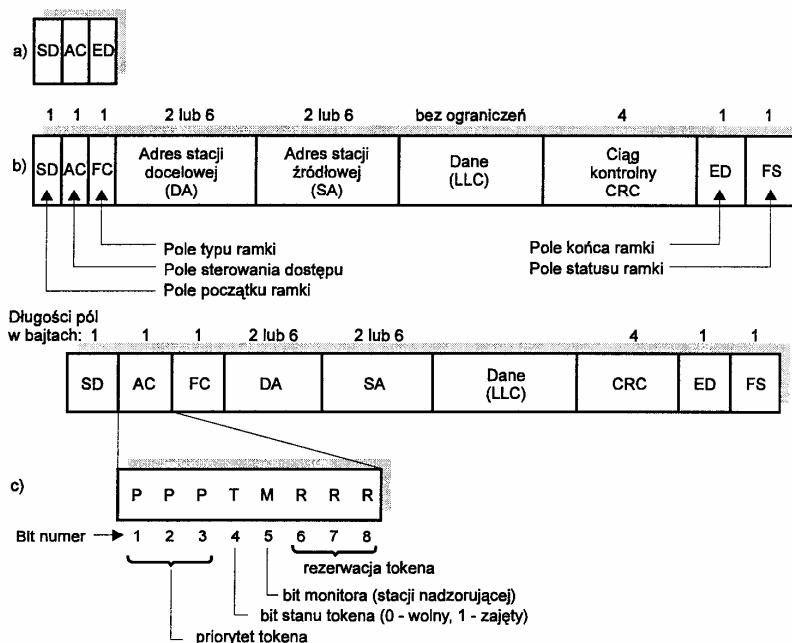
#### 4.2.3.2 Format ramki i tokena

W protokole MAC dla sieci pętlowej definiuje się niezależnie format tokena oraz zunifikowany format ramki. Formaty te ilustruje rysunek 4.28.

Przy braku zgłoszeń wymagających obsługi, wokół pętli krąży 3-bajtowy wolny token. W przypadku "zajęcia" tokena dwa pierwsze jego bajty tj. bajt początku

**tokena oraz bajt sterowania dostępem do medium** (ang. AC - Access Control) stają się dwoma pierwszymi bajtami (polami) ramki generowanej przez stację. Ostatnie pole tokena stanowi bajt jego końca, który w ramce występuje jako przedostatni. Znaczenie poszczególnych bitów pola sterowania dostępem AC jest następujące:

- 3 początkowe bity P określają priorytet tokena,
- bit czwarty T pozwala na identyfikację tokena lub ramki; gdy T=0 mamy do czynienia z wolnym tokenem, gdy T=1 token jest zajęty, a dwa jego pierwsze bajty stanowią początek ramki,
- piąty bit M wykorzystywany jest przez stację monitorującą i pozwala na identyfikację i usunięcie "bezpańskich" ramek,
- 3 ostatnie bity R służą do rezerwacji tokena o określonym przez pole R priorytecie.



Rys. 4.28. Struktury ramek w sieci IEEE 802.5: a) token, b) ramka informacyjna/sterująca, c) interpretacja bitów pola dostępu (AC) tokena/ramki

Trzecie pole ramki definiuje jej typ. Wyróżniamy przy tym ramki informacyjne, bądź kontrolno-sterujące ramki podwarstwy LLC oraz ramki utrzymywane sterujące, generowane przez podwarstwę MAC.

Przykładowe funkcje ramek utrzymywanych i ich typy podane są poniżej:

- zajęcie bądź żądanie tokena (CLAIM TOKEN) - oznaczające próbę przejęcia funkcji stacji monitorującej pracę pętli;
- potwierdzenie obecności potencjalnego/utajonego monitora (STAND BY MONITOR PRESENT) - przesyłane periodycznie i potwierdzające obecność potencjalnych stacji monitorujących;
- potwierdzenie obecności aktywnego monitora (ACTIVE MONITOR PRESENT) - przesyłane periodycznie przez stację pełniącą funkcję monitora pętli;
- przekazywanie informacji ostrzegawczej (BEACON) - wykorzystywane do lokalizacji przerwy w pętli;
- oczyszczanie pętli (PURGE) - stosowane do reinitjalizowania pętli i po przesłaniu ramki CLAIM TOKEN.

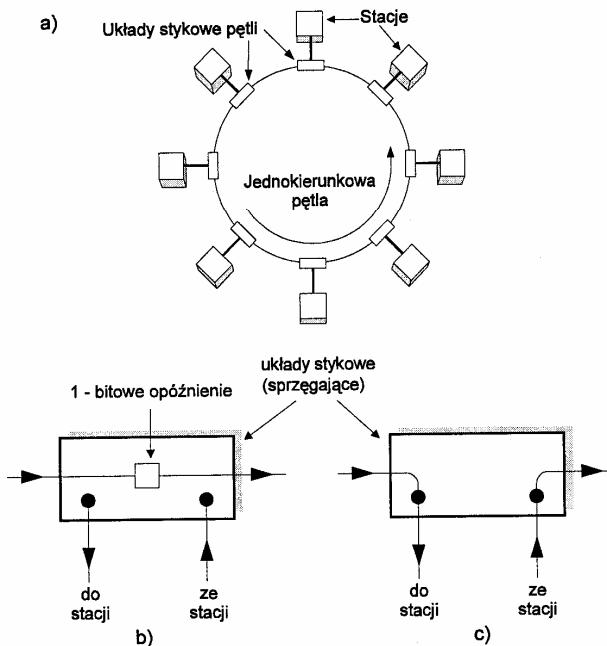
Kolejne dwa pola ramki zawierają adresy stacji źródłowej i docelowej. Podobnie jak w omawianych wcześniej standardach IEEE 802.3 i 802.4 mogą one być 16-sto lub 48-mio bitowe.

Pole danych, przygotowywane przez LLC, może mieć w IEEE 802.5 dowolną długość, ograniczoną jednakże w danej implementacji czasem posiadania tokena. Czas ten może być dla każdej stacji określony indywidualnie, najczęściej wynosi on około 10ms. Czterobajtowe pole zabezpieczenia CRC obejmuje wszystkie bajty ramki pojawiające się po polu startu. Dwa ostatnie pola ramki tj. pole jej końca (identycznie jak ostatni bajt tokena) oraz bajt statusu ramki (ang. FS - Frame Status) nie są objęte zabezpieczeniem CRC. Pole statusu ramki nie występowało we wcześniejszych formatach ramek standardów IEEE. Dwa bity tego pola, oznaczone jako A i C, są wykorzystywane do przesyłania powiadomień zwrotnych do stacji źródłowej ramki (por. typ 3 usługi oferowanej przez LLC). Stacja źródłowa, usuwająca z pętli wygenerowaną przez siebie ramkę, sprawdza bity A i C. Możliwe są trzy zasadnicze kombinacje mające następujące znaczenie:

- A=0 i C=0 - brak stacji docelowej w pętli, lub stacja wyłączona,
- A=1 i C=0 - brak akceptacji ramki przez stację docelową obecną w pętli,
- A=1 i C=1 - potwierdzenie odbioru ramki przez stację docelową.

W celu zwiększenia niezawodności pracy pętli bity A i C są w polu FS zdublowane. Dodatkowo, dla celów diagnostycznych, jeden z bitów pola końca ramki (pole przedostatnie) oznaczany jako bit E, wykorzystywany jest do sygnalizacji wykrycia błędów (np. wykrycie sygnału nie będącego elementem kodu Manchester). Informacja o wykrytej nieprawidłowości może być wprowadzona przez dowolną stację aktywną. Inny z bitów końca ramki służy z kolei do sygnalizacji zakończenia transmisji ciągu ramek (koniec przesyłanego zbioru).

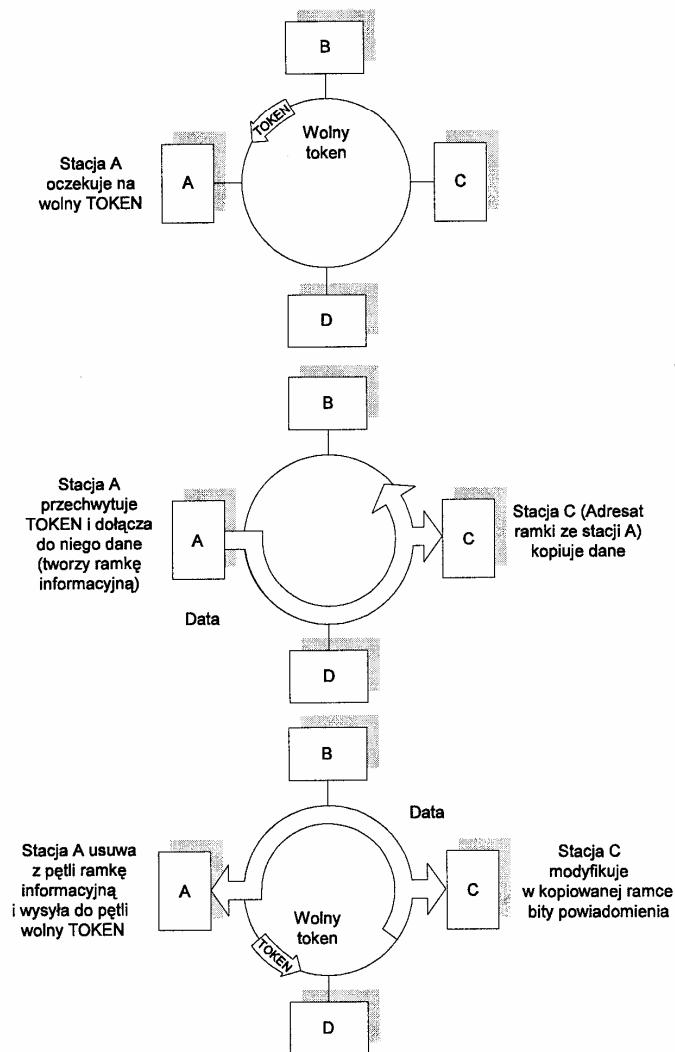
### 4.2.3.3 Procedury transmisji



Rys. 4.29. Ilustracja pracy sieci pętlowej: a) przykładowa sieć pętlowa, b) tryb nasłuchu, c) tryb transmisji

Jak wspomniano wcześniej, pętla stanowi zbiór połączeń punkt-punkt. Każdy bit napływający do interfejsu stacji, tj. układu sprzągającego stację z medium (magistralą), jest wprowadzany do bufora (co najmniej 1-no bitowego), a następnie ponownie wyprowadzony do magistrali. W czasie krótkiego przebywania w buforze ( $1/c$ , gdzie  $c = \text{szkość transmisji}$ ) każdy z bitów jest badany i ewentualnie modyfikowany. *Interfejs stacji może znajdować się w jednym z dwóch trybów pracy: nasłuchu (retransmisji napływających bitów) lub transmisji (wprowadzania własnych bitów do magistrali)*. W pierwszym trybie, ramki lub token przepływające przez układ stykowy są w nim jedynie opóźniane o 1 bit i retransmitowane. W drugim trybie, związanym z zajęciem tokena i transmisją ramki, ma miejsce przerwanie pętli, zgodnie z ilustracją pokazaną na rysunku 4.29. Opóźnienie 1-no bitowe w układzie stykowym pozwala stacji na przejście ze stanu nasłuchu do stanu transmisji. *Przy braku zgłoszeń wymagających obsługi, w pętli krąży nieustannie jeden wolny token* (z bitem  $T=0$ ). *Zajęcie tokena polega na zmianie wartości  $T$  z 0 na 1*. Konsekwencją tego jest też wspomniane powyżej przerwanie pętli i rozpoczęcie transmisji kolejnych pól ramki. Należy

przy tym podkreślić fakt, że *w dowolnej chwili tylko jedna stacja może przechwycić token i rozpocząć transmisję*. Przesyłanie ramek jest bezinterferencyjne, podobnie jak w 802.4, a kolejność w dostępie do magistrali wyznaczana jest w zasadzie przez położenie stacji (o ile pominiemy priorytety) w pętli fizycznej.



Rys. 4.30. Ilustracja przechwytywania tokena i przekształcanie go w ramkę informacyjną

**Stacja odbierająca wolny token może "przekształcić" go w ciąg ramek** (patrz rysunek 4.30). Z uwagi na realizowaną w pętli transmisję jednokierunkową, stacja wysyłająca ramkę ma obowiązek usunięcia jej z pętli (po pełnym obiegu) i wygenerowania nowego tokena z priorytetem tokena przechwyconego.

Wysłanie nowego tokena jest przy tym możliwe po spełnieniu dwóch warunków:

- stacja rozpoczęła odbiór i usuwanie z pętli swojej ramki

oraz

- zakończyła nadawanie ramki (bądź ciągu ramek).

Dopuszcza się tym samym jednoczesną obecność w pętli fragmentu ramki usuwanej właśnie przez stację i nowego „zregenerowanego” tokena.

Możliwe są też dwa inne scenariusze pracy stacji i pętli, a mianowicie:

- wysłanie wolnego tokena odbywa się dopiero po całkowitym usunięciu ramki (informacyjnej) z pętli (wersja z pojedynczą ramką w pętli),
- wysłanie wolnego tokena jest możliwe zaraz po zakończeniu wysyłania przez stację ramki (informacyjnej), tj. bez konieczności oczekiwania na jej powrót z pętli. W tym przypadku w pętli może pojawić się nawet kilka ramek (informacyjnych) i dokładnie jeden wolny token.

W ostatnim z prezentowanych scenariuszy (dopuszczenie wielu ramek krążących w pętli) strumień ramek może w sposób ciągły wypełniać pętlę. Rozwiązywanie to, nazywane metodą z wcześnieym uwalnianiem tokena (ang. *early TOKEN release*), jest szczególnie atrakcyjne w sieciach szybkich, o „długiej pętli” (tj. wnoszącej duże opóźnienia propagacyjne), a ponadto - gdy przesyłane są głównie krótkie ramki informacyjne (które mogłyby obniżyć efektywność wykorzystania medium). Omówiony wcześniej protokół tokenowy dla sieci magistralowej IEEE 802.4 definiował sposób utrzymania pętli logicznej jako całkowicie zdecentralizowany. W sieci pętlowej IEEE 802.5 zagadnienie to jest rozwiązywane odmiennie. **Każda pętla ma stację monitorującą jej pracę.** Jeżeli monitor ulega uszkodzeniu, jego funkcję przejmuję szybko inna stacja sieci (każda ze stacji ma przy tym możliwość stania się monitorem). Przejęcie funkcji monitora odbywa się zgodnie z pewną procedurą rywalizacji, po przesłaniu przez stacje ubiegające się o tę funkcję ramki CLAIM TOKEN. Jeżeli jedna ze stacji wyprzedzi inne stacje w transmisji tej ramki, to staje się ona stacją monitorującą.

**Do obowiązków aktywnego monitora należy:**

- **Kontrola obecności tokena w pętli.** Strata tokena jest wykrywana przez realizację procedury time-out-u, a monitor generuje nowy token.
- **Wykrywanie zniekształconych ramek.** Monitor wykrywa ramki o nie-właściwym formacie lub z błędą zawartością CRC i usuwa je z pętli.
- **Wykrywanie „bezpańskich” ramek.** Monitor wykrywa ramki nie usunięte przez stację źródłową. Odbywa się to poprzez ustawienie bitu M w polu AC i sprawdzenie tego bitu.

- **Lokalizacja przerw w ciągłości pętli.** Stacja aktywna, która zauważa niesprawność pętli, tj. stwierdza brak przepływu informacji ze stacji sąsiedniej, wysyła ramkę BEACON z podaniem własnego adresu (lub ewentualnego adresu stacji niesprawnej). Na podstawie odbioru napływających ramek BEACON i zawartych w nich adresów, stacja monitorująca ustala miejsce uszkodzenia i dokonuje zwarcia w układzie MAU odpowiedniego fragmentu pętli.

- **Wydłużanie czasu obiegu tokena.** W przypadku, gdy opóźnienie propagacyjne wnoszone przez magistralę plus opóźnienia w układach stykowych stacji są zbyt małe i nie pozwalają na umieszczenie całego tokena w pętli, stacja monitorująca wprowadza dodatkowe opóźnienie w pracy pętli. Zwróćmy uwagę na ciekawy fakt, że w wersji sieci 1 Mb/s sygnał odpowiadający 1 bitowi „rozciąga się” - biorąc pod uwagę zjawiska propagacyjne w magistrali - na długości ok. 250 m !

#### 4.2.3.4 Realizacja priorytetowego dostępu do pętli

Standard IEEE dopuszcza obsługę ramek o 8-miu priorytetach (od poziomu 0 - najniższego, do poziomu 7 - najwyższego) oraz możliwość rezerwacji tokena o odpowiednim priorytecie. Ramkom informacyjnym nadawane są priorytety od 0 do 6. Należy przy tym zwrócić uwagę na fakt, że w układach stykowych (adapterach) TMS 380C16, stosowanych w sieci IBM, liczba poziomów priorytetów jest ograniczona do sześciu.

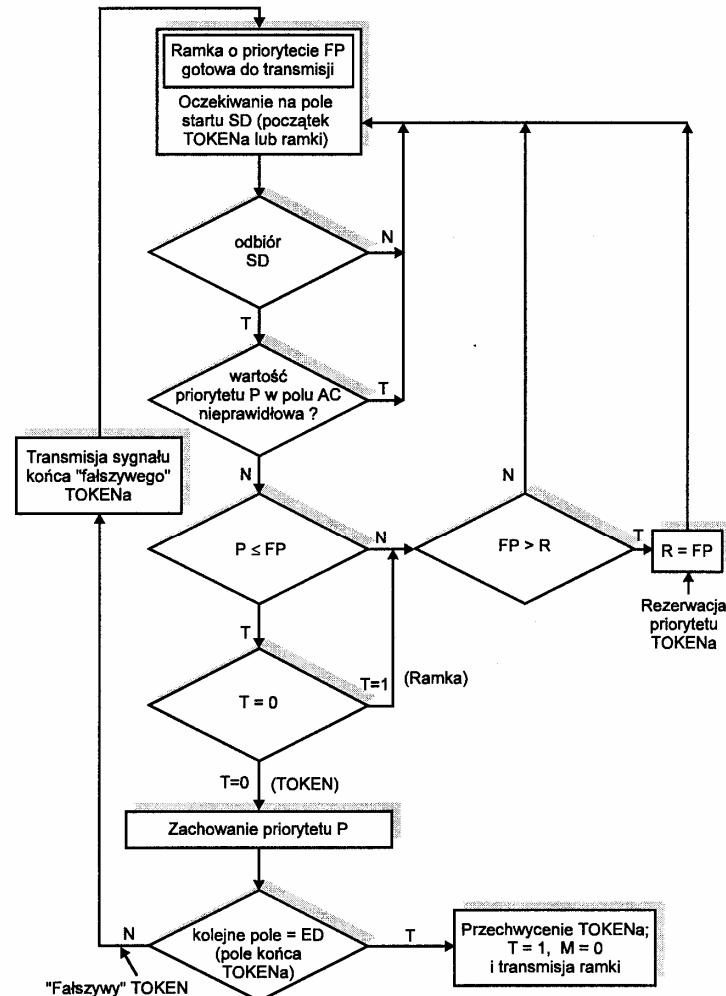
W procesie sterowania dostępem, obejmującym między innymi procedury rezerwacji tokena i modyfikacji jego aktualnego poziomu priorytetu P, wykorzystywane są poszczególne elementy pola AC sterowania dostępem do medium (z wyłączeniem bitu M zarezerwowanego do monitorowania pracy pętli). Działania podejmowane przez stację w przypadku zgromadzenia w buforze adaptera ramki F o priorytecie FP ilustruje rysunek 4.31.

Przykład rezerwacji i przydziału priorytetu zilustrowano na rysunku 4.32, wprowadzając następujące oznaczenia:

- FP - priorytet wiadomości (ramki) wymagającej transmisji,
- P - priorytet tokena (reprezentowany 3-bitowym ciągiem P w polu AC),
- R - poziom rezerwacji dokonywanej przez stację (zapisany na bitach R w polu AC).

1. Stacja pragnąca przesłać ramkę o priorytecie FP musi czekać na wolny token z  $P \leq FP$ .
2. Oczekując na token spełniający powyższy warunek, stacja może dokonać rezerwacji tokena o priorytecie FP. Dokonuje tego poprzez wpisanie na bitach R w polu AC tokena zajętego (stanowiącego początek transmitowanej ramki) wartość  $R=FP$  (o ile oczywiście w polu rezerwacji nie dokonano wcześniej zapisu wartości większej). Stacja usuwająca ramkę z pętli i generująca nowy token dokonuje przepisania bitów rezerwacji

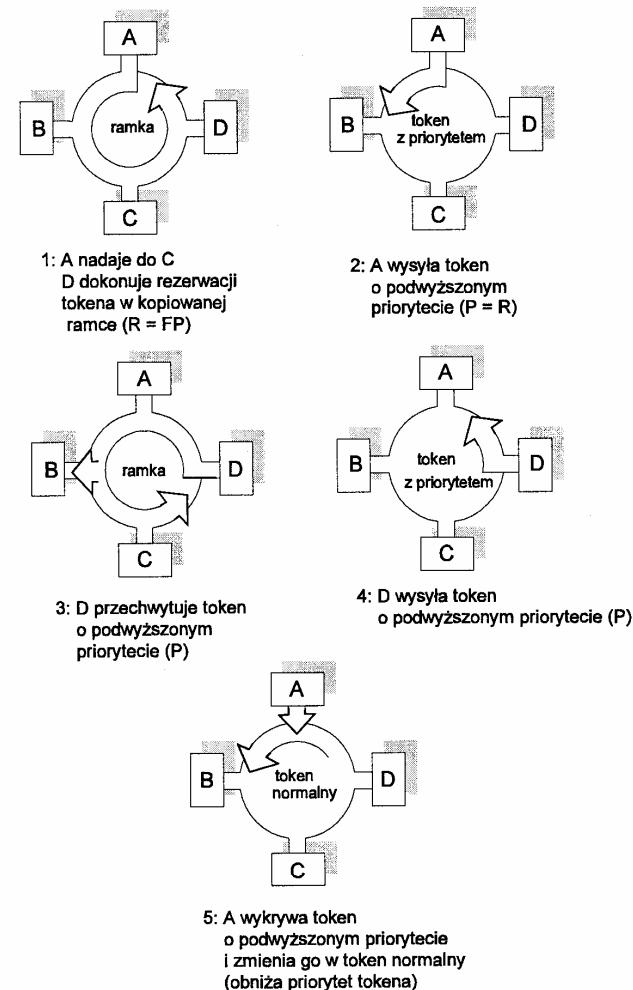
z pola R na pole bitów priorytetów tokena P. Tym samym wprowadzany do magistrali, zregenerowany token ma priorytet  $P=R=FP$ .



Rys. 4.31. Ilustracja procesu rezerwacji i przechwytywania tokena

3. Token o priorytecie P może zostać zajęty jedynie przez stację posiadającą wiadomość o identycznym priorytecie  $FP=P$ , w szczególności może to być stacja, która dokonała rezerwacji. Stacja ta zajmując token ustawia bit T jako 1.

4. Po transmisji stacja uwalnia token, pozostawiając jego priorytet P niezmieniony oraz zerując pole R.



Rys. 4.32. Algorytm transmisji i rezerwacji ramek w standardzie IEEE 802.5

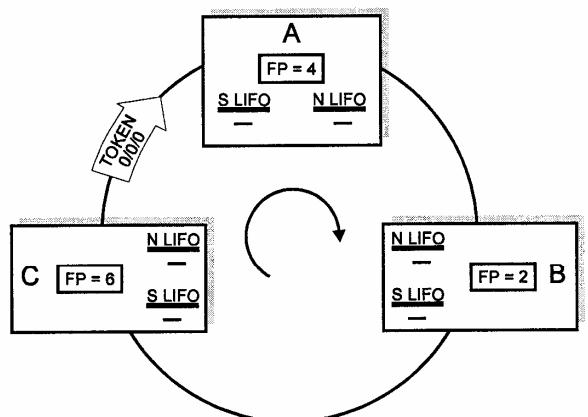
Powyższy algorytm powoduje podnoszenie priorytetu tokena. Ażeby uniknąć ograniczenia dostępu do magistrali wiadomościom o niższych priorytetach, stacja podnosząca priorytet tokena musi ten priorytet obniżyć do poziomu P przed operacją podnoszenia. Aby móc podwyższać lub obniżać priorytet, stacja ko-

rzysta z procedur stosowych. Każdy adapter sieciowy ma możliwość dokonania rezerwacji priorytetu tokena zgodnie z poziomem priorytetu FP ramki przygotowanej do transmisji, o ile tylko poziom ten jest wyższy od wartości R zapisywanej w polu AC tokena lub ramki. Proces nadzorowania priorytetu tokena odbywa się z wykorzystaniem automatu stanów (ang. *Priority Control State Machine*). Elementami tego automatu są:

- priorytetowy układ opóźniający oraz
- dwa bufore o dyscyplinie obsługi typu LIFO, nazywane odpowiednio nowym i starym buforem LIFO.

Priorytetowy układ opóźniający wprowadza 9-cio bitowe opóźnienie w adapterze stacji, pozwalające na dokonywanie ewentualnych modyfikacji priorytetu P w transmitowanym tokenie. **Z kolei nowy bufor LIFO (N LIFO)** jest w praktyce czterowarstwowym układem stosowym. Ostatnia warstwa, czy też ostatnia wprowadzona do bufora wartość to poziom priorytetu P, do którego został podniesiony priorytet tokena, i od którego począwszy automat stanów ma obniżać priorytet tokena. **Stary bufor LIFO (S LIFO)** jest również czterowarstwowym układem stosowym. Jego ostatnia wartość odpowiada poziomowi priorytetu, od którego automat stanów podniósł ostatnio poziom priorytetu tokena i do którego automat stanów ma obniżyć priorytet tokena.

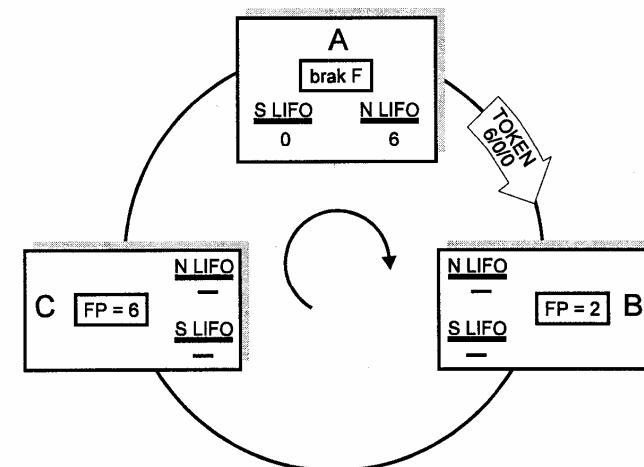
W adapterze stacji priorytetowy automat stanów współpracuje z układem sterowania transmisją tokena (ang. *Transmit Token Control State Machine*), odpowiadającym za funkcje rezerwacji priorytetu tokena.



Rys. 4.33. Ilustracja początkowego stanu sieci i lokalizacji tokena

Zasadę realizacji algorytmu priorytetowego dostępu do pętli omówimy na przykładzie sieci z 3-ma aktywnymi stacjami oznaczonymi dalej jako A, B i C. Przyjmijmy przy tym, że:

- stacja A ma przygotowaną do transmisji ramkę o dowolnym priorytecie, np. FP=4;
- stacja B ma przygotowaną do przesłania ramkę o priorytecie FP=2;
- stacja C ma przygotowaną do przesłania ramkę o priorytecie FP=6;
- początkową lokalizację tokena o zerowym priorytecie P=0 (bity PPP w polu AC) i o zerowej zawartości pola rezerwacji (zerowe bity RRR w polu AC) ilustruje rysunek 4.33;
- stan tokena (ewentualnie ramki po przejęciu tokena) charakteryzowany jest trójką liczb P/T/R oznaczających poziom priorytetu, stan tokena (T=0 - token, T=1 - ramka) i poziom rezerwacji.

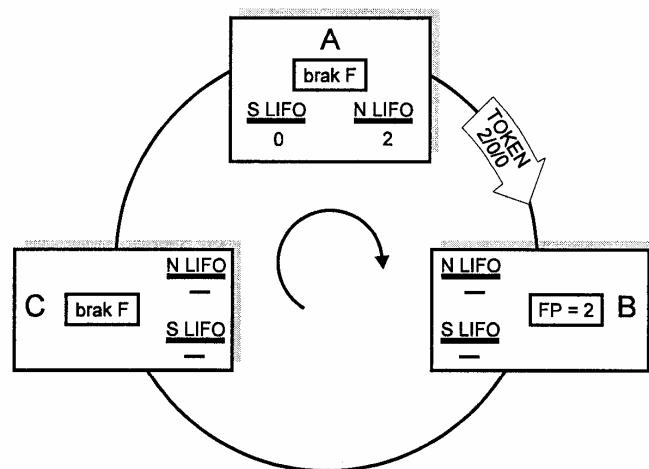


Rys. 4.34. Ilustracja stanu sieci po jego uwolnieniu przez stację A

Kolejne fazy w pracy sieci, w rozważanym przykładzie będą następujące:

1. po przejęciu tokena przez stację A, stacja ta przekształca go w ramkę bez modyfikacji bitów priorytetu i rezerwacji. Stan ramki opisany będzie jako 0/1/0 (P=0, T=1, R=0);
2. stacje B i C dokonują kolejno modyfikacji rezerwacji tokena o priorytecie - odpowiednio - 2, w przypadku stacji B, i 6, w przypadku stacji C;
3. stacja A usuwa swoją ramkę z pętli i uwalnia nowy token o podwyższonym priorytecie: 6/0/0; modyfikuje też zawartości buforów S LIFO i N LIFO; ilustruje to rysunek 4.34;
4. stacja B nie może przejąć tokena, gdyż FP<P (FP=2, P=6); stacja dokonuje kolejnej rezerwacji tokena; tym samym pole AC tokena na wyjściu stacji B ma postać 6/0/2;

5. token zostaje przejęty przez stację C, która przekształca go w ramkę 6/1/2;
6. ramka po obiegu wokół pętli zostaje z niej usunięta przez stację C; stacja ta uwalnia też nowy token z polem AC o postaci 6/0/2;
7. token 6/0/2 po dotarciu do stacji A podlega procedurze modyfikacji poziomu priorytetu P (zgodnie z zasadą pracy "priorytetowego" automatu stanów); wartość 6 zapamiętana w buforze N LIFO zostaje zmieniona na wartość 2, a uwolniony token przyjmuje postać 2/0/0; stan sieci i buforów LIFO ilustruje rysunek 4.35.
8. token 2/0/0 zostaje przejęty przez stację B; w przypadku braku pakietów do transmisji w stacjach A i C ramka z polem AC 2/1/0 obiega wokół pętli bez modyfikacji tego pola; stacja B po usunięciu ramki z pętli uwalnia token 2/0/0;
9. po dotarciu tokena 2/0/0 do stacji A i po porównaniu jego priorytetu P=2 z ostatnią wartością bufora N LIFO, następuje przywrócenie pierwotnego, zerowego priorytetu tokena (wartość z S LIFO);
10. stacja A uwalnia bezpriorytetowy token z polem 0/0/0, bufore N LIFO i S LIFO stacji A zostają wyzerowane, sieć powraca do stanu „zero-wego”.



Rys. 4.35. Ilustracja stanu sieci i TOKENa po jego dotarciu do stacji A i realizacji procedur modyfikacji priorytetu

#### 4.2.3.5 Ocena jakości pracy sieci pętlowej

Dokonując przybliżonej analizy pracy sieci opisanej standardem IEEE 802.5, przyjmiemy, że:

1. wszystkie stacje dysponują ramkami gotowymi do transmisji (duże obciążenie stacji);
2. w systemie nie stosuje się priorytetów;
3. nowy token może być wygenerowany po zakończeniu transmisji ramki i rozpoczęciu jej odbioru z pętli;
4. układy stykowe stacji wprowadzają 1-bitowe opóźnienia, a stacje rozłożone są równomiernie wokół pętli;
5. czas transmisji tokena jest pomijalnie mały w stosunku do czasu trwania ramki.

Ponadto przyjmiemy następujące oznaczenia:

N	- liczba stacji w pętli,
$\tau = L / C$	- całkowite opóźnienie propagacyjne w pętli,
T=F/c	- czas transmisji ramki,
$\Delta = \frac{1}{c} + \frac{\tau}{N}$	- opóźnienie wnoszone przez pojedynczy segment pętli.

Rozważmy dwa przypadki pracy sieci pętlowej związane ze stosowaniem ramek „długich” bądź „krótkich”.

**Ramki długie:**  $T > \tau + N \frac{1}{c}$

W tym przypadku token zostaje uwolniony natychmiast po zakończeniu transmisji ramki. Wykorzystanie kanału wynosi więc

$$U = \frac{T}{T + \Delta}$$

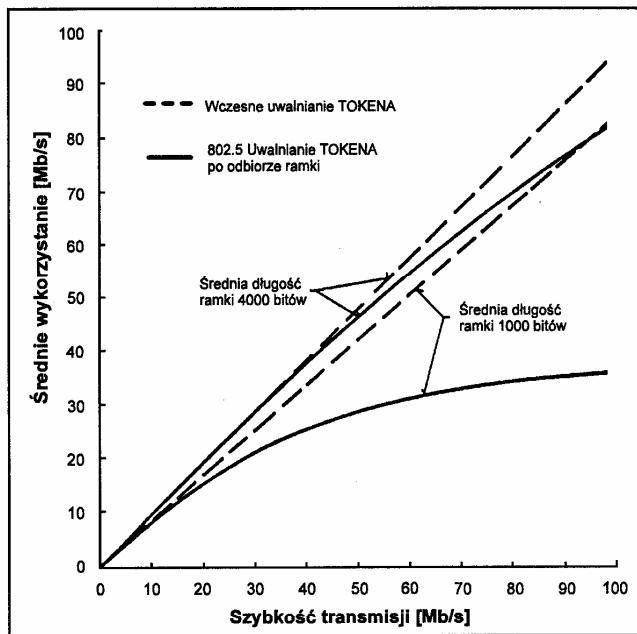
**Ramki krótkie:**  $T < \tau + N \frac{1}{c}$

W przypadku ramek krótkich uwolnienie tokena ma miejsce po czasie nie krótszym niż  $N\Delta$ . Tym samym U ma postać:

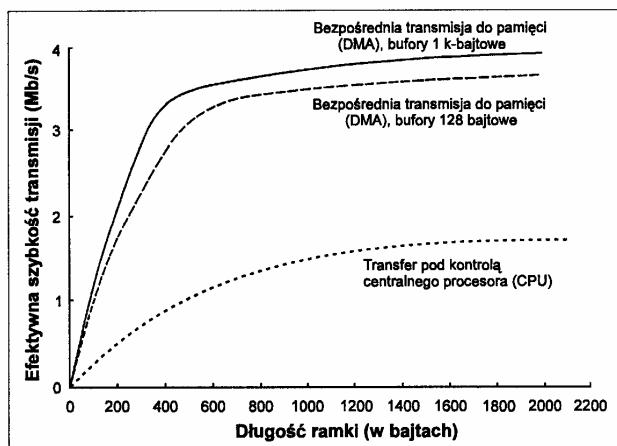
$$U = \frac{T}{\tau + N \frac{1}{c} + \Delta}.$$

W pracy sieci pętlowej możemy też dopuścić tzw. wczesne (szybkie) uwalnianie tokena (jedna z opcji IEEE 802.5) polegające na wprowadzeniu nowego tokena do magistrali natychmiast po zakończeniu transmisji ramki. Porównanie zmian wykorzystania kanału U (tutaj: efektywnej szybkości transmisji) w rozwiązaniach z normalnym i z wczesnym uwalnianiem tokena w funkcji szybkości transmisji c z przedziału od 0 do 100 Mb/s dla różnych średnich długości ramek przedstawione jest na rysunku 4.36 (zauważmy przy tym, że szybkości powyżej 16 Mb/s nie są realizowane w standardowych rozwiązaniach Token Ring).

Z kolei na rysunku 4.37 pokazano zmiany efektywnej szybkości transmisji w funkcji długości ramek (w bajtach) dla różnych rodzajów przesyłanych wiadomości w sieci IBM z szybkością transmisji 4 Mb/s.

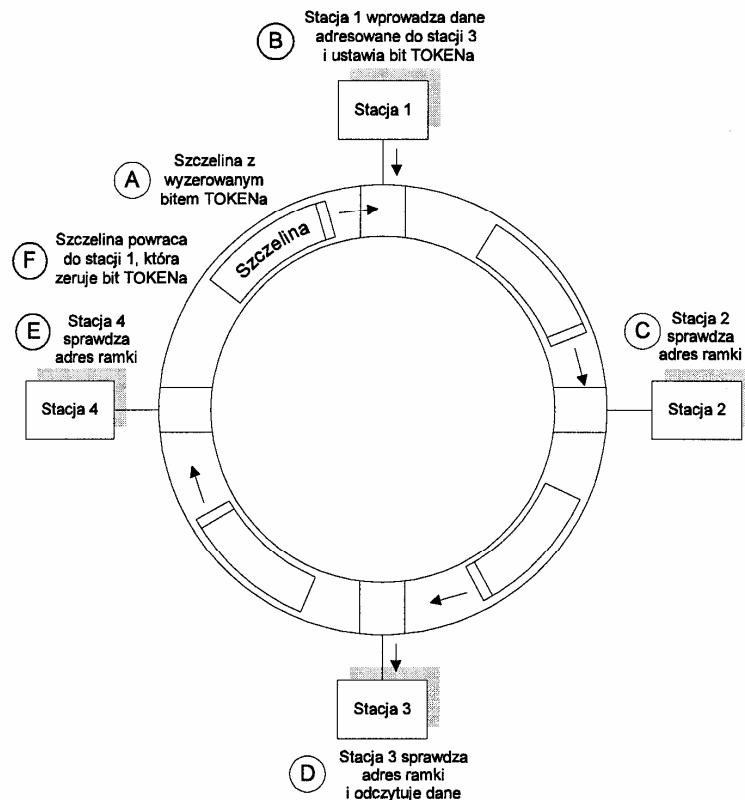


Rys. 4.36. Zależność średniego wykorzystania kanału od szybkości transmisji w pętli, w przypadku wcześniego lub normalnego uwalniania tokena



Rys. 4.37. Zmiany efektywnej szybkości transmisji w funkcji długości ramek dla różnych rodzajów wiadomości przesyłanych w sieci IBM o szybkości pracy 4 Mb/s

#### 4.2.4 Protokół dla sieci pętlowej z wirującymi szczelinami (ramki)

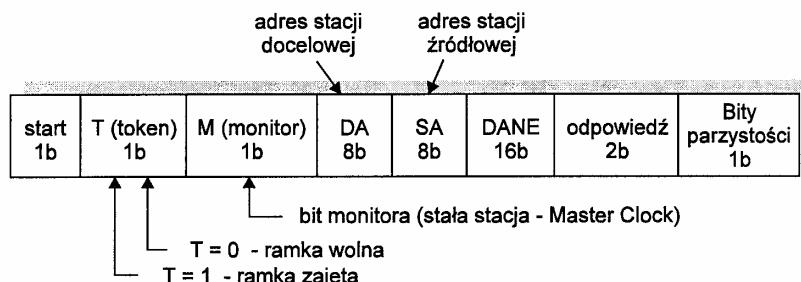


Rys. 4.38. Ilustracja pracy sieci pętlowej z wirującymi szczelinami (ramkami)

Przekazywanie tokena jako znacznika regulującego dostęp do medium nie jest jedyną metodą dostępu stosowaną w pętlowych sieciach LAN. Innym *rozwiązaniem, znajdującym szerokie zastosowanie praktyczne, jest tzw. pierścień szczelinowy, nazywany też Cambridge Ring lub slotted Ring*. W rozwiąaniu tym, ilustrowanym na rysunku 4.38, czas obiegu pętli  $T_c$  przez sygnał fizyczny ( $T_c$  obejmuje opóźnienie propagacyjne w kablu oraz opóźnienia wprowadzone przez układy stykowe stacji) dzielony jest na miniszzelinys czasowe o czasie trwania równym czasowi transmisji pojedynczego bitu. Podział cyklu  $T_c$  na miniszzelinys pozwala na wprowadzenie do pętli pewnej (zwykle większej od 1) liczby ramek o stałej długości, które krążą w postaci wirujących szczelin czasowych wokół pętli. W przypadku, gdy fizyczna długość pętli jest niewystarczająca

do pomieszczenia kilku ramek, układy stykowe wprowadzają dodatkowe opóźnienia sygnałów elementarnych. W przypadku sieci Cambridge Ring o szybkości transmisji 10 Mb/s ze 100 stacjami rozlokowanymi w odległościach 10 m, na obwodzie pierścienia można "zmieścić" ponad 150 bitów. Pozwala to na organizację czterech ramek po 38 bitów każda.

*Krążące wokół pętli ramki przypominają pociągi składające się z lokomotyw i wagonów. "Lokomotywami" są przy tym części nagłówkowe ramek zawierające w szczególności bity charakteryzujące zajętość ( $T=1$ ) lub swobodę ( $T=0$ ) "pociągu"/ramki. Stacja mająca do przesłania informację musi czekać na wolny "pociąg", tj. ramkę z nagłówkiem (minitokenem) o wartości  $T=0$ . Struktura ramki w sieci Cambridge Ring pokazana jest na rysunku 4.39. W przypadku, gdy wolna ramka dociera do stacji zmieniony zostaje jej status, poprzez wpisanie bitu  $T=1$ . Do pozostałych elementów wirującej ramki przepisana zostaje stosowna informacja.*



Rys. 4.39. Struktura ramki MAC w sieci Cambridge Ring (poszczególne pola ramki mają długości wyrażone w bitach)

W przeciwieństwie do postaci ramek w IEEE 802.5 ramki w pierścieniu szczelinowym są bardzo krótkie. Regeneracja ramki, tj. zmiana jej statusu z zajętej na wolną oraz zerowanie pól informacyjnych dokonywane jest (podobnie jak w IEEE 802.5) przez stację źródłową. Zerowanie to ma jednakże charakter "logiczny" tj. bez konieczności usuwania nadanej ramki z pętli. Należy też zwrócić uwagę na fakt, że metoda dostępu z wirującymi szczelinami (ramkami) zapewnia:

- (1) bardzo wysoką sprawność wykorzystania pętli, bliską jedności przy dużym obciążeniu (z maksymalnym efektywnym wykorzystaniem medium  $U=D/F$ ),
- (2) sprawiedliwy dostęp do medium oraz
- (3) ograniczony maksymalny czas dostępu do medium.

Podobnie jak w sieci pętlowej opisanej standardem IEEE 802.5, w rozwiążaniu Cambridge Ring istnieje możliwość przesyłania natychmiastowych powiadomo-

mień. Służą do tego dwa bity odpowiedzi ustawiane przez stację docelową. Ich interpretacja jest przy tym następująca:

- 00 - stacja nie dysponuje zasobami pozwalającymi na odbiór ramki (brak wolnych buforów stacji),
- 01 - ramka została skopiowana,
- 10 - ramka została celowo odrzucona,
- 11 - brak stacji o adresie wskazanym w ramce; kombinacja 11 stanowi jednocześnie wartość początkową bitów pola odpowiedzi.

Sprawiedliwość dostępu do medium reguluje zasada mówiąca, że zajęcie przez stację kolejnej ramki na transmisję danych może mieć miejsce dopiero po oznaczeniu wcześniej nadanej ramki jako wolnej (po modyfikacji bitu T z 1 na 0).

Analogicznie do algorytmów pracy sieci IEEE 802.5 *szereg funkcji sterujących utrzymywanych realizowanych jest przez wyznaczoną (tutaj na stałe) stację monitorującą*. Do zadań monitora (ang. *Master Clock*) należy między innym:

- synchronizacja pracy pętli, a w szczególności nadzorowanie szybkości transmisji bitów/ramek,
- ustalanie wymaganej "długości bitowej" pętli oraz
- usuwanie "bezpańskich" ramek krążących wokół pętli (zmiana ich statusu logicznego).

#### 4.2.5 Protokół dostępu do sieci pętlowej z rejestrami przesuwającymi

Innym, nieco bardziej skomplikowanym rozwiążaniem sieci pętlowej LAN jest wersja z rejestrami przesuwającymi, czy też rejestrami wtrąconymi do pętli (ang. *Register Insertion Ring*). Zasadę pracy stacji takiej sieci ilustruje rysunek 4.40. Każda stacja posiada dwa bufore. Pierwszy z nich jest rejestrzem przesuwającym, służącym do odbioru napływających do stacji, lub kierowanych poprzez nią ramek. Drugi bufor wykorzystywany jest do czasowego przechowywania ramek generowanych przez daną stację. Ramki przesyłane w sieci mogą mieć przy tym zmienną długość, ograniczoną jednakże rozmiarem bufora nadawczego (wyjściowego). W momencie rozpoczęcia pracy przez stację rejestr przesuwający oraz bufor nadawczy są puste. W przypadku bufora odbiorczego (rejestru przesuwającego) definiowany jest wskaźnik określający komórkę rejestru, do której należy wprowadzić element odbieranej ramki. Wskaźnik ten w chwili rozpoczęcia pracy wskazuje prawą skrajną komórkę rejestru. Z chwilą rozpoczęcia odbioru ramki z pętli, kolejne bity wprowadzane są do odpowiednich komórek rejestru, przy czym wskaźnik przesuwa się każdorazowo o jedną pozycję w lewo. W momencie zgromadzenia w buforze/rejestrze części adresowej ramki (z adresem stacji docelowej) stacja podejmuje decyzję, czy odebrana ramka jest kierowana do tej stacji, czy też nie. Jeżeli tak, to ramka zostaje wprowadzona do bufora wewnętrznego stacji, a wskaźnik zajętości rejestru ustawiony zostaje w prawej skrajnej pozycji. Zazwyczaj w rozwiążaniu tym,

odmiennie jak w IEEE 802.5, to stacja docelowa, a nie źródłowa "oczyszczająca" pętlę. Należy przy tym zaznaczyć, że w pętlowej sieci LAN z rejestrami przesuwającymi dopuszcza się też opcję z usuwaniem ramki przez jej stację źródłową.



Rys. 4.40. Ilustracja dostępu do sieci pętlowej z rejestrami przesuwającymi

*Jeżeli odebrana ramka jest ramką tranzytową, to po stwierdzeniu tego faktu rozpoczyna się proces jej ponownego wprowadzania do pętli, z jednoczesnym odbiorem kolejnych elementów ramki.* Wskaźnik komórki rejestru nie ulega wówczas modyfikacji do chwili odbioru ostatniego bitu ramki, gdy zaczyna się on przesuwać w prawo, osiągając prawe skrajne położenie w chwili zakończenia wysyłania ramki.

Proces transmisji ramki wygenerowanej przez daną stację może mieć miejsce, gdy:

- (1) ramka przygotowana do transmisji znajduje się w buforze wyjściowym stacji,
- (2) liczba wolnych komórek (odpowiadających liczbie szczelin) w rejestrze przesuwnym jest nie mniejsza niż długość ramki gotowej do transmisji.

Jedynie wtedy, gdy oba warunki są spełnione, ma miejsce przełączenie klucza (por. rys. 4.40) przyłączającego bufor wyjściowy do pętli (bądź też równolegle przepisanie bufora wyjściowego do rejestru przesuwającego) i wyekspediowanie ramki. W przypadku, gdy podczas transmisji ramki lokalnej rozpocznie się odbiór innej ramki, wówczas kolejne jej bity są wprowadzane do bufora wejściowego (rejestru przesuwającego). Natychmiast po zakończeniu transmisji ramki z bufora wyjściowego ma miejsce przełączenie klucza i rozpoczęcie obsługi ramki zgromadzonej w buforze wejściowym.

Interesującą właściwością sieci pętlowej z rejestrami przesuwającymi jest fakt zapobiegania monopolizacji medium przez jedną stację. W przypadku, gdy po zakończeniu wysyłania ramki (tranzytowej) z magistrali nie jest

odbierana kolejna ramka, wówczas rejestr przesywny stacji będzie pusty. Tym samym stacja może rozpocząć przesyłanie swojej własnej ramki. Oznacza to, że przy braku ramek napływających magistralą stacja może wykorzystywać całą przepustowość medium. Jednakże w przypadku zajętości magistrali, stacja po wysłaniu jednej ramki własnej nie będzie mogła dokonać transmisji ramki kolejnej, z uwagi na brak odpowiedniej liczby wolnych komórek w odbiorczym rejestrze przesywnym (por. warunek (2)). Należy pamiętać, że wysłanie ramki o długości a-bitów wiąże się z koniecznością istnienia a-komórkowej wolnej przestrzeni w rejestrze wejściowym.

*Protokół dostępu do magistrali w sieci pętlowej z rejestrami przesuwającymi pozwala na uzyskanie 100%, a nawet wyższej (!) sprawności wykorzystania medium.* Sformułowanie to brzmi nieco paradoksalnie. Należy jednakże pamiętać o tym, że w wersji dopuszczającej usuwanie ramki z pętli przez stację docelową, istnieje możliwość przesłania nawet kilku ramek informacyjnych w czasie pojedynczego cyklu pracy pętli. Oznacza to wielokrotne wykorzystanie wspólnego medium transmisyjnego. Podobny mechanizm i podobną efektywność pracy możemy zaobserwować w sieci DQDB (sieci MAN IEEE 802.6) w wersji z węzłami wymazującymi.

Wadą rozwiązania protokołarnego z oczyszczaniem pętli przez adresata jest jednakże brak możliwości przesyłania szybkich powiadomień MAC.

W rozwiązaniu z rejestrami przesuwającymi konieczne jest (podobnie jak w systemach pętlowych omawianych poprzednio) wyznaczenie stacji MONITORA nadzorującej pracę pętli.

#### 4.2.6 Szybkie sieci LAN

Wraz z rozwojem systemów czasu rzeczywistego i pojawieniem się różnorodnych aplikacji multimedialnych rośnie zapotrzebowanie na zwiększenie szybkości transmisji w sieciach LAN. Stosowane do tej pory standardy 10 megabitowego Ethernetu (IEEE 802.3), czy 16 megabitowego Token Ringu (IEEE 802.5) stają się niewystarczające. Jedną z przesłanek, którymi kierowano się przy projektowaniu nowych systemów sieci lokalnych, było zapewnienie możliwości funkcjonowania ogromnej liczby stacji komputerowych połączonych skrętką (10Base-T i częściowo sieci typu Token Ring). Z kolei dobrze opanowana technologia ethernetowa skierowała wysiłki standaryzacyjne w kierunku modyfikacji tego standardu w taki sposób, aby stało się możliwe wykorzystanie go do przesyłania informacji z większymi szybkościami.

W tym paragrafie książki omówimy dwa nowe standardy umożliwiające transmisję z szybkościami 100 Mb/s. Standardami tymi, wykorzystującymi częściowo lub w pełni idee Ethernetu, są:

- standard IEEE 802.12 (wersja komercyjna - 100VG-AnyLAN), który może być zaimplementowany w dotychczasowej infrastrukturze (okablowaniu) sieci LAN oraz

- standard 100BaseX oparty na rozwiązaniu IEEE 802.3.

#### 4.2.6.1 100VG-AnyLAN

100VG-AnyLAN jest rozwiązaniem łączącym infrastrukturę sieciową, opracowaną przez AT&T i Hewlett Packarda, z oprogramowaniem firm Novell, Microsoft, AT&T, Hewlett Packard oraz kilkunastu innych dostawców. Jako medium transmisyjne wykorzystuje on, podobnie jak Ethernet 10Base-T, skrętkę 3 kategorii. Odmiennie jednakże od techniki CSMA/CD (Ethernet), 100VG-AnyLAN korzysta z nowej priorytetowej metody dostępu, określanej mianem priorytetowego dostępu na żądanie (ang. *demand priority*). Zgodnie z koncepcją firmy Hewlett Packard, to format ramki, a nie protokół dostępu, jest czynnikiem decydującym o możliwości współpracy odmiennych standardów sieciowych. Technologia 100VG-AnyLAN umożliwia więc transmisję ramek Ethernetu (IEEE 802.3) i Token Ringu (IEEE 802.5) z szybkościami 100 Mb/s (w pierwszych wersjach 100VG-AnyLAN dopuszciano jedynie ramki Ethernetu). Istniejące okablowanie, spełniające wymagania 10Base-T i Token Ringu, można bez zmian wykorzystać przy migracji do szybkiej sieci 100VG-AnyLAN. Ta nowa technologia, zapewniając kompatybilność swoich ramek z ramkami sieci 802.3 i 802.5, nie wymaga też zmian ani sieciowego systemu operacyjnego, ani oprogramowania użytkowego. Do układu huba 100VG-AnyLAN można dołączyć zarówno komputer pracujący w tym standardzie, jak też sieć 10Base-T. W rozwiązaniu 100VG-AnyLAN oprócz formatu ramek, ze standardu 802.3, zachowano też charakterystyczną dla rozwiązania 10Base-T gwiaździstą topologię sieci i identyczną zasadę okablowania strukturalnego. Używane są również takie same złącza jak w 10Base-T. Wspomniana kompatybilność ramek i okablowania zezwala także na połączanie (za pośrednictwem mostu) sieci 100VG-AnyLAN do istniejących sieci Ethernet lub Token Ring. Stosując zaś routery można spręgać segmenty 100VG-AnyLAN z magistralą FDDI, ATM oraz z sieciami WAN.

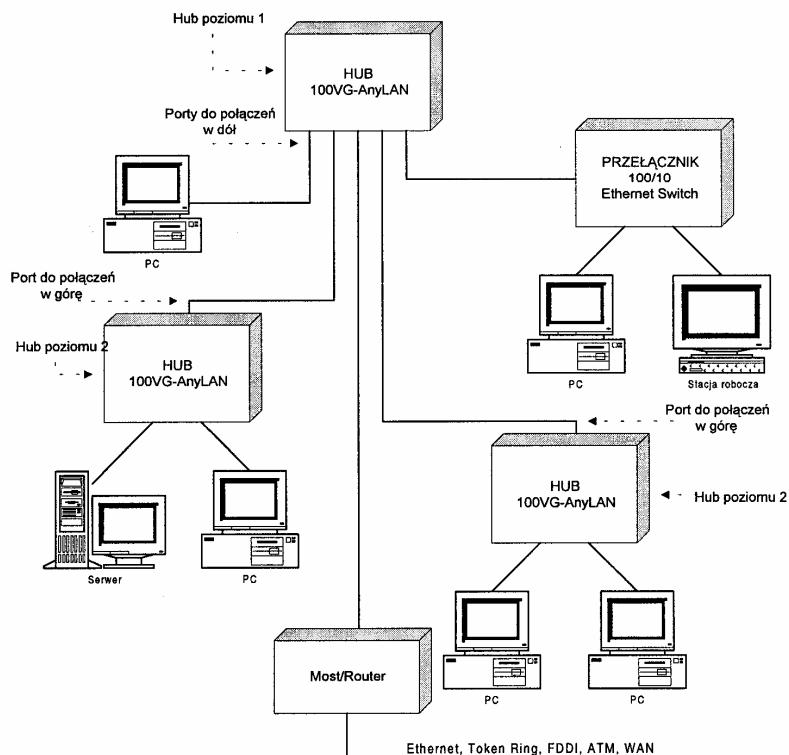
##### 4.2.6.1.1 Struktura sieci 100VG-AnyLAN

Ogólna struktura sieci 100VG-AnyLAN pokazana jest na rysunku 4.41. Charakteryzuje się ona topologią fizycznej gwiazdy, której środkiem jest hub (zwany hubem centralnym, hubem poziomu pierwszego lub rootem). Wyklucza się więc tworzenie jakichkolwiek pętli fizycznych. Zasadniczymi elementami tej sieci są:

- co najmniej jeden hub 100VG-AnyLAN,
- co najmniej jedna stacja sieciowa,
- połączenia sieciowe,
- opcjonalne urządzenia sieciowe (np. routery, mosty, przełączniki).

Od huba poziomu pierwszego odchodzą połączenia do innych węzłów (huby poziomu drugiego itd.), te z kolei mogą dalej rozgałęziać sieć lub podłączać stacje końcowe. Oczywiście do huba poziomu pierwszego można także podłączać stac-

je końcowe (np. PC). Ponadto, jak pokazane to jest na rysunku, sieć 100VG-AnyLAN przystosowana jest do współpracy z innymi sieciami za pomocą mostów i routerów. Na rysunku 4.41 pokazano sposób łączenia sieci 100VG-AnyLAN z sieciami Ethernet, Token Ring, FDDI, ATM i WAN. Przedstawiono także sposób kaskadowego łączenia hubów. Węzłem sieci 100VG-AnyLAN może być komputer PC, występujący w roli klienta lub serwera, stacja robocza lub dowolne z urządzeń sieciowych takich jak: przełącznik, most, router lub hub 100VG-AnyLAN. Chociaż dopuszcza się istnienie do 1024 "węzłów", to zalecana liczba urządzeń nie powinna przekraczać 250. Narzucone są też stosowne ograniczenia na np. liczbę mostów między dwoma węzłami ( $\leq 7$ ). Sieć 100VG-AnyLAN może być dzielona na segmenty przy użyciu mostów, przełączników lub routerów. Huby 100VG-AnyLAN mogą być łączone ze sobą kaskadowo bez potrzeby stosowania jakichkolwiek urządzeń pośredniczących. Zakłada się przy tym możliwość tworzenia trzydziestostopniowej kaskady hubów.



Rys. 4.41. Ogólna struktura sieci 100VG-AnyLAN

Założono, że 100VG-AnyLAN wykorzystuje te same kable co rozwiązańe 10Base-T. Ponieważ są to przewody telefoniczne, do zapewnienia niezawodnej transmisji o szybkości 100 Mb/s, konieczna okazała się transmisja „kwartetowa”. O ile więc w 10Base-T wykorzystywane są dwie pary przewodów (jedna do nadawania, druga do odbioru), to w 100VG-AnyLAN używa się czterech par (w zasadzie do pracy półduplekowej).

Zgodnie ze specyfikacją sieć 100VG-AnyLAN powinna umożliwić stosowanie następujących rodzajów kabli:

- 4-parowe kable nieekranowane UTP 3, 4 i 5 kategorii,
- 2-parowe kable ekranowane (IBM Typ 1),
- kable światłowodowe.

#### 4.2.6.1.2 Hub 100VG-AnyLAN

Centralnym układem sieci 100VG-AnyLAN jest hub 100VG-AnyLAN. Pełni on rolę kontrolera zarządzającego dostępem do sieci poprzez ciągłe wykonywanie szybkiego skanowania (zgodnie z metodą „round robin”) swoich portów w celu sprawdzenia żądań obsługi dołączonych do niego węzłów. Hub otrzymuje dane i kieruje je bezpośrednio na port skojarzony z adresem docelowym pakietu danych.

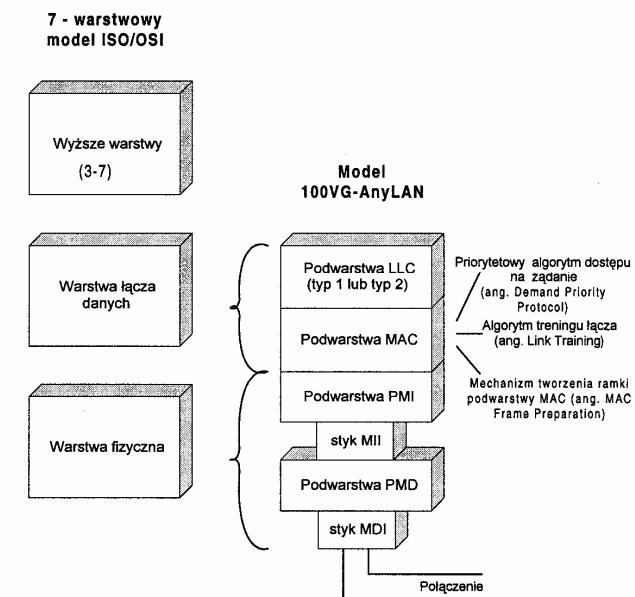
Wszystkie urządzenia sieciowe są podłączane do tego huba za pośrednictwem jego portów. Hub 100VG-AnyLAN jest wyposażony w dwa rodzaje portów (patrz rysunek 4.41) - porty do połączeń w dół i porty do połączeń w góre. Pierwsze z nich umożliwiają podłączanie stacji sieciowych (którymi mogą być serwery, stacje robocze oraz inne urządzenia sieciowe takie jak mosty, routery, przełączniki) lub hubów niższego poziomu, a drugie - opcjonalne - pozwalają na połączenie hubów niższego poziomu z hubami wyższego poziomu (powstaje wówczas kaskada hubów).

Każdy port huba może pracować w dwóch trybach: normalnym i monitorowania. W trybie normalnym port przepuszcza tylko te pakiety, które są adresowane do węzła skojarzonego z danym portem, natomiast w trybie monitorowania port przepuszcza wszystkie pakiety docierające do huba. Konfiguracja trybu normalnego czy monitorowania może być włączona automatycznie lub zainicjowana przez stację końcową.

#### 4.2.6.1.3 Model ISO/OSI a standard 100VG-AnyLAN

Przedmiotem opisu standardu 100VG-AnyLAN są warstwy WŁD - łącza danych i WF - fizyczna (patrz rysunek 4.42). W standardzie 100VG-AnyLAN warstwa fizyczna zawiera dwie podwarstwy:

- podwarstwę fizyczną niezależną od medium - PMI (ang. *Physical Medium Independent*) oraz
- podwarstwę fizyczną zależną od zastosowanego medium - PMD (ang. *Physical Medium Dependent*).



Rys. 4.42. 100VG-AnyLAN a 7-warstwowy model ISO-OSI

Z warstwą fizyczną związane są również dwa układy stykowe:

- interfejs łączący podwarstwę PMI z podwarstwą PMD - MII (ang. *Medium Independent Interface*),
- interfejs będący złączem między podwarstwą PMD, a kablem - MDI (ang. *Medium Dependent Interface*).

Zadaniem warstwy WF jest zapewnienie transmisji bitów między dwiema stacjami sieciowymi, czyli terminalami, serwerami, komputerami osobistymi, hubami, mostami, itp.

Warstwa WŁD w standardzie 100VG-AnyLAN dzieli się również na dwie podwarstwy:

- podwarstwę kanału logicznego (Sterowania Łączem Logicznym) LLC (ang. *Logical Link Control*) i
- podwarstwę dostępu do medium (Sterowania Dostępnem do Medium) MAC (ang. *Media Access Control*).

W podwarstwie MAC realizowane są mechanizmy:

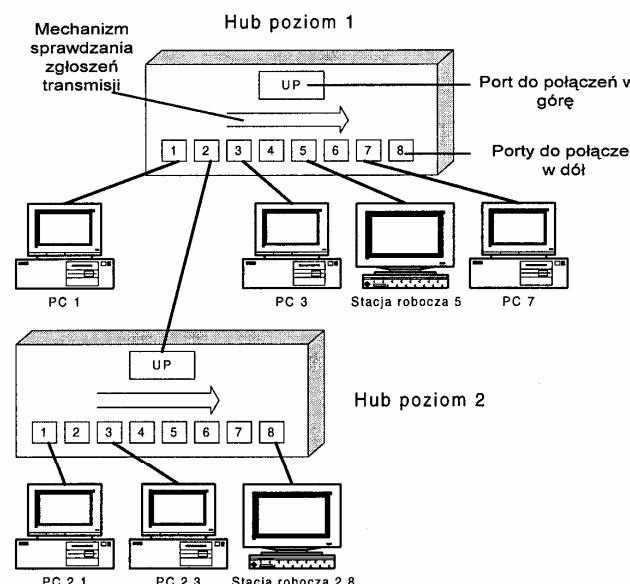
- priorytetowego dostępu do medium na żądanie DPP (ang. *Demand Priority Protocol*),
- treningu połączenia (ang. *Link Training*),

- przygotowania ramki MAC (ang. *MAC Frame Preparation*).

#### 4.2.6.1.4 Priorytetowy dostęp do medium

Metodą dostępu stosowaną w technologii 100VG-AnyLAN jest priorytetowy dostęp do medium na żądanie DPP. Zgodnie z DPP, stacja sieciowa gotowa do transmisji danych przesyła do huba 100VG-AnyLAN sygnał żądania transmisji. Sygnał ten może mieć normalny lub wysoki (podwyższony) priorytet. Jeśli stacja jest w stanie nieaktywnym, wysyła sygnały "Idle" (brak aktywności). Hub w sposób sekwencyjny, począwszy od najniższego numeru portu, sprawdza, które z podłączonych do niego urządzeń zgłaszały gotowość do transmisji. Sekwencja sprawdzania kończy się na najwyższym, wykorzystywanym, numerze portu. Dla normalnych priorytetów żądań transmisji hub obsługuje żądania w kolejności numerów portów. Jeśli występuje żądanie o wysokim priorytecie, to zostaje ono obsłużone w pierwszej kolejności.

Dla zilustrowania mechanizmu DPP posłużymy się opisany poniżej przykładem działania sieci przedstawionej na rysunku 4.43.



Rys. 4.43. Ilustracja realizacji metody DPP

Założmy, że do portów 2, 3, 5, 7 huba poziomu 1 napłynęły sygnały żądania transmisji o normalnym priorytecie i hub ten jest w trakcie obsługi żądania transmisji pochodzącego od PC 1. Do portów 1, 3, 8 huba poziomu 2 również dotarły żądania transmisji o normalnym priorytecie.

Ponieważ wszystkie zgłoszone żądania transmisji mają jednakowy - normalny - priorytet, to hub poziomu 1 będzie je obsługiwał zgodnie z rosnącą numeracją portów. Proces "przepływu" będzie się odbywał zgodnie z zasadą round-robin w następującej kolejności:

1. **PC 1** - Hub poziomu 1 obsługuje zgłoszenie żądania transmisji od komputera PC 1.
2. **PC 2.1** - Hub poziomu 1 obsługuje zgłoszenie żądania transmisji napływające do portu 2. Port 2 huba poziomu 1 jest połączony z hubem poziomu 2. W momencie, gdy hub poziomu 1 rozpozna, że do jego portu 2 jest połączony inny hub, następuje przekazanie sterowania do huba poziomu 2. Hub poziomu 2 obsługuje wtedy żądania transmisji od swoich portów, zgodnie z numeracją portów. Ponieważ pierwsze w kolejności numerów portów jest żądanie od komputera PC 2.1, ono właśnie zostaje obsłużone jako pierwsze.
3. **PC 2.3** - Hub poziomu 2 kontynuuje obsługę swoich zgłoszeń, tym samym następne w kolejności obsługi jest żądanie od komputera PC 2.3.
4. **Stacja Robocza 2.8** - Analogicznie jak wyżej ma miejsce obsługa kolejnego żądania od stacji roboczej 2.8.
5. **PC 3** - Ponieważ wszystkie zgłoszenia żądania obsługi pochodzące z huba poziomu 2 zostały obsłużone, hub poziomu 1 przechodzi do obsługi swojego kolejnego portu, na którym pojawiło się żądanie transmisji, a więc do portu 3, do którego jest połączony komputer PC 3.
6. **Stacja robocza 5** - Hub poziomu 1 przechodzi do obsługi kolejnego portu, tzn. portu 5, do którego jest dołączona stacja robocza 5.
7. **PC 7** - Kolejnym obsługiwany przez hub poziomu 1 portem jest port 7, do którego połączony jest komputer PC 7.

Jeżeli w sytuacji podobnej do opisanej powyżej stacja robocza 2.8 zgłosiła żądanie transmisji o wysokim priorytecie, wówczas żądanie to hub poziomu 2 przekazuje do huba poziomu 1. Ten z kolei będzie wtedy obsługiwał żądania w następującej kolejności:

1. **PC 1** - Hub poziomu 1 obsługuje żądania transmisji od komputera PC 1. Nie przerywa tej obsługi i załatwia ją do końca.
2. **Stacja Robocza 2.8** - Następuje obsługa żądania transmisji o wysokim priorytecie pochodzącego od stacji roboczej 2.8.
3. **PC 2.1** - Po obsłudze żądania o wysokim priorytecie następuje powrót do obsługi żądań o normalnym priorytecie, czyli obsługi, pierwszego w kolejności numerów portów, komputera PC 2.1 - huba poziomu 2 dołączonego do portu 1.
4. **PC 2.3** - Analogicznie jak w poprzednim przypadku, hub poziomu 2 dalej obsługuje swoje zgłoszenia, przechodząc do obsługi żądania pochodzącego od komputera PC 2.3.

5. PC 3 - Ponieważ wszystkie żądania transmisji pochodzące od portów huba poziomu 2 zostały obsłużone, hub poziomu 1 przechodzi do obsługi kolejnego portu, na którym pojawiło się żądanie transmisji, a więc do portu 3, do którego jest podłączony komputer PC 3.
6. Dalej obsługiwane są: stacja robocza 5 i komputer PC 7 - analogicznie jak w poprzednim przypadku.

Metoda DPP poprawia efektywność pracy sieci przez eliminację kolizji występujących w sieci Ethernet i opóźnień w przekazywaniu tokena, charakterystycznych dla sieci Token Ring. Z kolei, używanie jednego priorytetu dla transmisji danych, a innego dla zastosowań multimedialnych gwarantuje dostęp do sieci nawet najbardziej wymagającym aplikacjom, takim jak np. wideokonferencje. Jednakże aby nie dopuścić do zmonopolizowania dostępu do sieci przez zgłoszenia o podwyższonym priorytecie, po czasie około 200 - 300 ms obsługi tych zgłoszeń (odmierzany przez licznik huba), hub dokonuje automatycznego podwyższenia priorytetu zgłoszeń normalnych. Tym samym obsługa wszystkich zgłoszeń zaczyna odbywać się w identyczny sposób.

#### 4.2.6.1.5 Trening połączenia

Kolejną ważną funkcją zdefiniowaną w podwarstwie MAC jest funkcja o nazwie trening połączenia (ang. *Link Training*). Funkcja ta przygotowuje hub i podłączoną do niego stację sieciową do transmisji. Przygotowanie to polega na określeniu adresu stacji sieciowej i sprawdzeniu poprawności funkcjonowania układów stykowych i kabla łączącego hub ze stacją sieciową.

6	6	2	2	580-675	4
Adres docelowy (same zera)	Adres stacji źródłowej (zera w przypadku hubów)	Żądana konfiguracja (określa status węzła - informacja przesyłana z węzła do huba)	Dopuszczalna konfiguracja (określa konfigurację sieci - informacja wysyłana z huba do węzła sieci)	Dane (informacja protokołarna)	Pole kontrolne FCS

Rys. 4.44. Struktura ramki treningowej standardu IEEE 802.12

W trakcie działania funkcji Link Training, hub i stacja sieciowa wymieniają między sobą tzw. ramki treningowe (ang. *training frames*). Struktura takich ramek pokazana jest na rysunku 4.44. Jeżeli wymiana ramek przebiega poprawnie, to pozwala to na pozytywne zweryfikowanie połączenia między hubem a stacją sieciową. W czasie, gdy między dowolnym hubem, a stacją sieciową jest realizowana funkcja Link Training, ramki treningowe są wysyłane także do innych hubów po to, by powiadomić je, że w sieci przebiega taki proces.

Mechanizm treningu połączenia automatycznie dostarcza hubowi informacji o wszystkich stacjach sieciowych do niego dołączonych. Ramki wysyłane przez stację w czasie procesu Link Training i odbierane przez hub, zawierają informacje o:

#### 4.2.6 Szybkie sieci LAN

- Typie urządzenia - (hub, stacja sieciowa, router, itd.).
- Trybie pracy urządzenia, w tym rodzaju zaimplementowanego "mechanizmu" bezpieczeństwa (normalny lub mieszany).
- Adresie MAC-owym stacji.

Gdy stacja sieciowa zostaje podłączona do huba po raz pierwszy, mechanizm Link Training danej stacji automatycznie inicjuje wysyłanie do huba sygnałów informujących o tym fakcie (sygnały treningu jałowego - *Idle*).

#### 4.2.6.1.6 Przygotowanie ramki MAC

Trzecim mechanizmem zdefiniowanym w podwarstwie MAC (patrz rys. 4.42) jest mechanizm przygotowania ramki MAC (ang. *MAC Frame Preparation*). Jest on odpowiedzialny za dodawanie do każdej ramki przesyłanej do warstwy fizycznej, adresu źródłowego i adresu docelowego oraz sekwencji kontrolnej ramki FCS (ang. *Frame Check Sequence*).

Standard 100VG-AnyLAN umożliwia obsługę, przez podwarstwę MAC, trzech formatów ramek. Są to ramki:

- Ethernemu (IEEE 802.3),
- Token Ringu (IEEE 802.5) i
- ramki specjalne dla realizacji mechanizmu Link Training (definiowane w specyfikacji IEEE 802.12).

Sieci 100VG-AnyLAN są homogeniczne. Oznacza to, że pojedynczy segment tej sieci może pracować tylko w jednym formacie ramki (tzn. nie może jednocześnie obsługiwać ramek Ethernet i Token Ring). Jeżeli więc w sieci 100VG-AnyLAN stacja sieciowa pracująca w segmencie z formatem ramek Ethernet wymaga komunikacji ze stacją sieciową pracującą w segmencie z formatem ramek Token Ring, to między tymi segmentami musi być zainstalowany most tłumaczący Ethernet - Token Ring.

Standard 100VG-AnyLAN umożliwia łączenie segmentów Ethernetu o szybkości 10 Mb/s z segmentami 100VG-AnyLAN, stosującymi ramki Ethernemu. W takim przypadku pomiędzy łączonymi segmentami instalujemy most dopasowujący szybkości transmisji w obu podsieciach. Ilustruje to rysunek 4.41.

Możliwe jest również połączenie sieci Token Ring 16 lub 4 Mb/s z segmentem 100VG-AnyLAN o ramce Token Ringu. W obu tych przypadkach, do łączenia dwóch segmentów wykorzystuje się proste mosty.

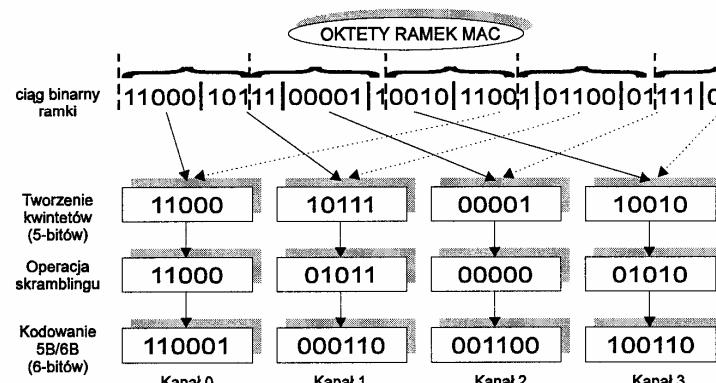
#### 4.2.6.1.7 Podwarstwa PMI

PMI jest górną podwarstwą warstwy fizycznej (patrz rys. 4.42). Jest ona niezależna od stosowanego w sieci medium. Dzięki podwarstwie PMI przetwarzanie ramek przebiega zawsze tak samo (niezależnie od zastosowanego okablowania sieci).

W przypadku gotowości podwarstwy PMI do transmisji, przejmuje ona oktety (ośmiobitowe jednostki informacji) z podwarstwy MAC i przygotowuje ramki do

transmisji przez medium fizyczne, dodając ciągi preambuły i znaczniki początku i końca ramki.

Z kolei, gdy PMI odbiera ramkę z podwarstwy PMD, to przed jej przesłaniem do podwarstwy MAC usuwa wprowadzone przez warstwę fizyczną elementy organizacyjne.



Rys. 4.45. Przykład przekształcania ciągów binarnych ramek w sekstyty kodu 5B/6B, po uprzednim podziale na kwintety i ich skramblingu

Podwarstwa PMI realizuje, w trakcie nadawania, funkcje zilustrowane na rysunku 4.45. Funkcje te obejmują:

- Konwersję oktetów MAC-owskich na kwintety i rozdział kwintetów na cztery strumienie (w technologii 100VG-AnyLAN korzystamy przy transmisji z czterech par przewodów - cztery kanały - z których każdy przesyła część informacji). Oktety ramki MAC widziane jako ciągi bitów są dzielone na grupy 5-ciobitowe i kierowane do 4 kanałów.
- Mieszanie (skrambling) 5-bitowych „kwintetów”. Proces ten polega na stosowaniu oddzielnego generatora liczb przypadkowych w odniesieniu do każdego kanału. Pozwala to eliminować powtarzanie się samych zer lub jedynek.
- Kodowanie 5B/6B. Kodowanie 5-bitowych ciągów, zawartych w kwintetach po skramblingu, za pomocą 6-bitowych sekstetów. Proces ten pozwala uzyskać tzw. zrównoważone struktury danych, mające pożądaną liczbę zer i jedynek, i gwarantujące tym samym synchronizację odbiorników, a w konsekwencji - ich niezawodną pracę. Dzięki temu mechanizmowi możliwe jest wychwytywanie błędów związanych z symbolami i strukturami nieuprawnionymi. Kodowanie 5B/6B pozwala uzyskać szybkość przesyłania informacji w jednej parze 25 Mb/s, przy szybkości modulacji jedyne 30 MBodów, co daje 83% wykorzystanie przepustowości całego łącznika.

- Dalsze formowanie ramki w celu przygotowania pakietu do transmisji przez warstwę PMD (dodanie preambuły, znacznika początku i końca ramki).

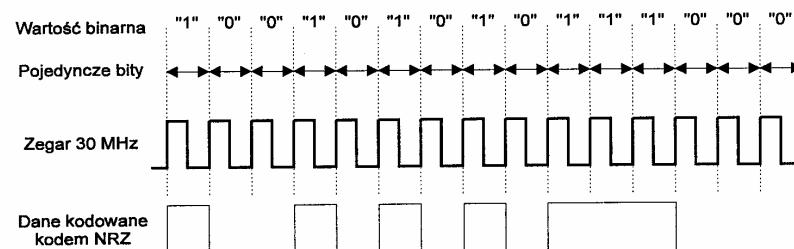
Transmisja danych w typowym rozwiązaniu 100VG-AnyLAN przebiega pół-dupleksowo. Wynika to z faktu, że wszystkie cztery pary skrętki (w przypadku stosowania skrętki 4 UTP) są wykorzystywane jednocześnie. Ramki/ciągi sygnalizacyjne w 100VG-AnyLAN mogą być przekazywane w trybie pełndupleksowym. Do ich transmisji w jednym kierunku wykorzystywane są bowiem jedynie dwie pary skrętki.

#### 4.2.6.1.8 Warstwa PMD

Zadania dolnej części warstwy fizycznej, tj. podwarstwy PMD, zależnej od rodzaju stosowanego medium, obejmują:

- multipleksowanie kanałów - w przypadku użycia jako medium transmisyjnego 2 parowej skrętki czy światłowodu,
- kodowanie typu NRZ (ang. *Non Return to Zero*),
- badanie stanu medium połączeniowego i kontrola statusu połączeń.

Kodowanie NRZ (1 - stan wysoki, 0 - stan niski; transmitowany jest jeden bit danych na jeden cykl zegarowy) przedstawione jest na rysunku 4.46.



Rys. 4.46. Ilustracja procesu kodowania NRZ w sieciach 100VG-AnyLAN

Przy transmisji danych w sieci 100VG-AnyLAN wykorzystującej 4-parową skrętkę UTP stosuje się zegar o częstotliwości 30 MHz. Pozwala to na transmisję z szybkością modulacji 30 MBodów przez każdy z 4 kanałów. Ze względu na stosowanie kodowania 5B/6B efektywna szybkość transmisji wynosi 25 Mb/s w jednym kanale. Stąd łącznie, w 4 kanałach, uzyskuje się przepływność 100 Mb/s (4 x 25 Mb/s).

Transmisje w medium mogą być organizowane zarówno w trybie pełno- jak i pół-dupleksowym.

Tryb pełndupleksowy stosowany jest do wymiany informacji dotyczących kontroli statusu połączeń (ang. *Link - Status Control*). Z kolei w trybie półdupleksowym przesyłane są ramki informacyjne kierowane z węzła do huba lub odwrotnie.

Do kontroli statusu połączeń wykorzystywane są kombinacje ciągów binarnych o dwóch częstotliwościach:

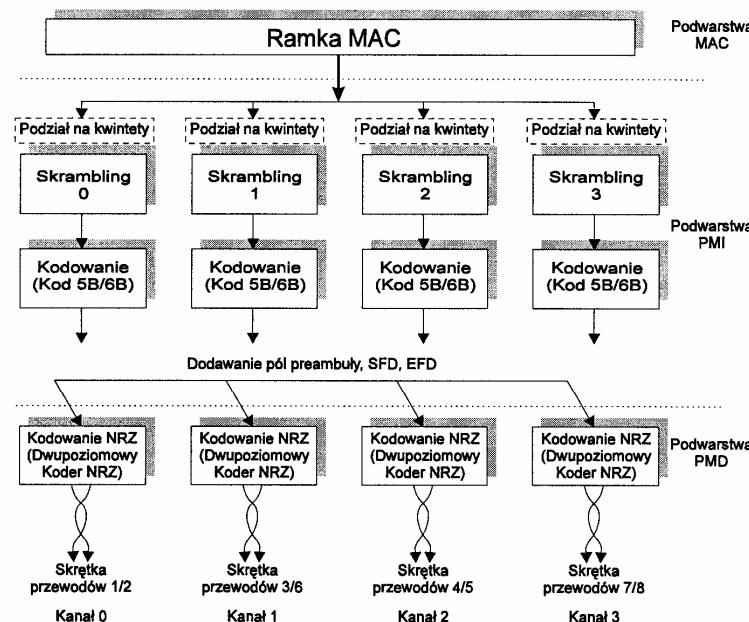
- sekwencje szesnastu zer a po nich - szesnastu jedynek, dające, dla zegara 30 MHz, częstotliwość 0.9375 MHz (30 MHz/32 bity), określana jako Ton1,
- sekwencje ośmiu zer, a po nich - ośmiu jedynek, dające, dla zegara 30 MHz, częstotliwość 1.875 MHz (30 MHz/16 bitów), określana jako Ton2,

Sekwencje sygnałów wysyłane pomiędzy stacją a hubem i odwrotnie zamieszczone zostały w tabeli 4.3.

Tabela 4.3. Sekwencje sygnałów wykorzystywanych do kontroli statusu połączeń

Transmitowana sekwencja	Znaczenie sygnałów w przypadku odebrania przez węzeł (stację roboczą)	Znaczenie sygnałów w przypadku odebrania przez hub
Ton 1 - Ton 1	bezczytny (Idle)	bezczytny (Idle)
Ton 1 - Ton 2	pakiet danych przychodzących	żądanie obsługi z normalnym priorytetem
Ton 2 - Ton 1	dochodzące nie zdefiniowane - do wykorzystania w przyszłości	żądanie obsługi z wysokim priorytetem
Ton 2 - Ton 2	żądanie wywołania procedur Link - Training	żądanie wywołania procedur Link - Training

odbiór sygnału „bezczytny (Idle)” – oznacza:  
dla stacji - hub nie ma żadnych pakietów oczekujących na transmisję,  
dla huba - brak żądań obsługi napływających ze stacji.



Rys. 4.47. Ilustracja procedur realizowanych w sieci 100VG-AnyLAN w przypadku wykorzystania 4-ro parowej skrętki UTP

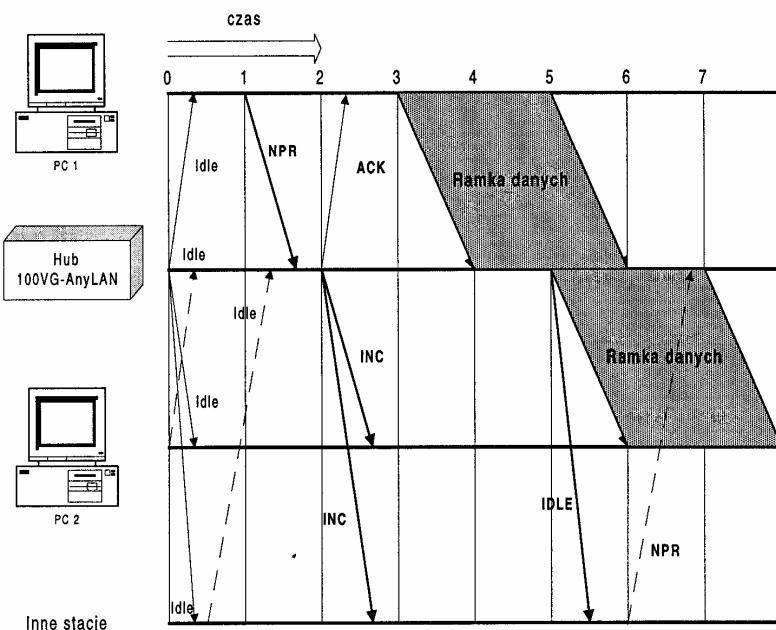
Procedury realizowane w poszczególnych podwarstwach warstwy fizycznej (WF) sieci 100VG-AnyLAN w przypadku stosowania 4-ro parowej skrętki UTP, pokazano na rysunku 4.47.

#### 4.2.6.1.9 Przykładowy przebieg transmisji danych w sieci 100VG-AnyLAN

W przypadku sieci 100VG-AnyLAN definiuje się 3 podstawowe rodzaje rozwiązań. Są to:

- sieci z jednym poziomem hubów i 4-ro parową skrętką (4 UTP),
- sieci wielopoziomowe ze skrętką 4 UTP,
- sieci ze skrętką 2 STP lub kablem światłowodowym.

Przykładowy przepływ danych między dwoma komputerami - PC 1 - stacja nadawcza, PC 2 - stacja odbiorcza - zainstalowanymi w sieci z jednym hubem 100VG-AnyLAN i kablem 4 UPT (transmisja danych w sieci z jednym poziomem hubów i 4-ro parową skrętką UTP) przedstawiony jest na rysunku 4.48.

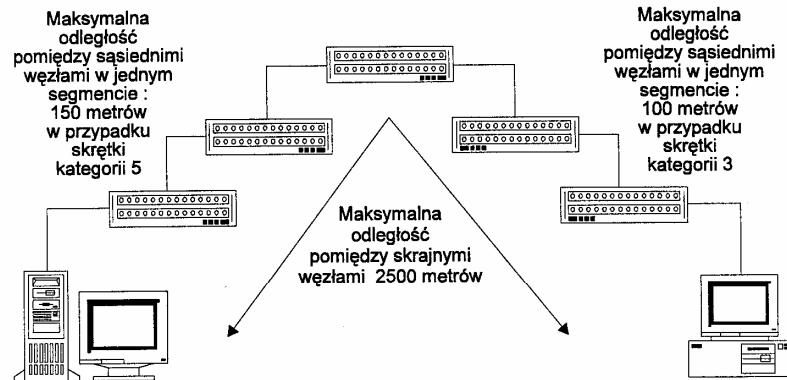


Rys. 4.48. Transmisja danych w sieci 100VG-AnyLAN

Działania podejmowane przez stacje lub hub w kolejnych fazach przepływu danych, odpowiadających ilustracji z rysunku 4.48, są przy tym następujące:

- t = 0 - Sieć jest w stanie „spoczynku”. Hub 100VG-AnyLAN wysyła sygnały „Idle” do wszystkich podłączonych stacji. Sygnały „Idle” są także wysyłane przez stacje sieciowe.
- t = 1 - Stacja nadawcza - PC 1 - wysyła sygnał "normalnego priorytetu" NPR (ang. *NPR - Normal Priority Request* - transmitowana sekwencja: Ton1 - kanałem 2 i Ton2 - kanałem 3) do huba, żądając pozwolenia na transmisję ramki o normalnym priorytecie. Hub po stwierdzeniu, że stacja żąda transmisji, wstrzymuje wysyłanie do niej sygnałów „Idle” (Idle - Ton1 kanałami 0 i 1), co powoduje, że kanały stacji PC 1 zostają odblokowane. Następnie do stacji źródłowej zostaje wysłany sygnał potwierdzenia (ACK), a do pozostałych stacji, do których pakiet może być przeznaczony, wysyłany jest sygnał INC (ang. *INComing* – transmitowana sekwencja: Ton1 - kanałem 0 i Ton2 - kanałem 1).
- t = 2 - Hub 100VG-AnyLAN przesyłając sygnał INC powiadamia wszystkie potencjalne stacje odbiorcze o możliwości przesłania do nich ramki. Umożliwia to stacji odbiorczej przyjęcie ramki na wszystkich czterech kanałach (czterech parach skrętki). Równocześnie stacja PC 1, po stwierdzeniu, że jej interfejs jest wolny, przygotowuje się do transmisji danych, przesyłając ramkę z podwarstwy MAC do podwarstwy PMI. Podwarstwa PMI w PC 1 rozdziela, w opisany w poprzednim podrozdziale sposób, dane na cztery strumienie, miesza je, a następnie zamienia w 6 - bitowe symbole, według zasady kodowania 5B/6B. Ramka po uzupełnieniu jej o znacznik początku SFD (ang. *Start Frame Delimiter*) i znacznik końca ramki EFD (ang. *End Frame Delimiter*), zostaje przesłana do podwarstwy PMD.
- t = 3 - Podwarstwa PMD w PC 1 rozpoczyna wysyłanie ramki do huba.
- t = 4 - Hub odbiera ramkę i dekoduje adres stacji odbiorczej (w naszym przypadku PC 2).
- t = 5 - Ramka jest przesyłana do stacji sieciowej o zdekodowanym adresie przeznaczenia (PC 2).
- t = 6 - Hub zaprzestaje wysyłania sygnału „INC” i rozpoczyna wysyłanie sygnału „Idle” do wszystkich pozostałych urządzeń (nie zostało to ujęte na rysunku), trwa przesyłanie ramki do PC 2.
- t = 7 - Koniec wysyłania ramki do stacji PC 2.
- t = 8 - Stacja PC 2 po odbiorze całej ramki rozpoczyna wysyłanie sygnału „Idle”.

W przypadku standardu 100VG-AnyLAN mamy możliwość zastosowania do 5 hubów pomiędzy skrajnymi węzłami. Odległość pomiędzy skrajnymi węzłami nie może być przy tym większa niż 2,5 km. Ilustrację łączenia stacji w sieci 100VG-AnyLAN przedstawia rysunek 4.49.



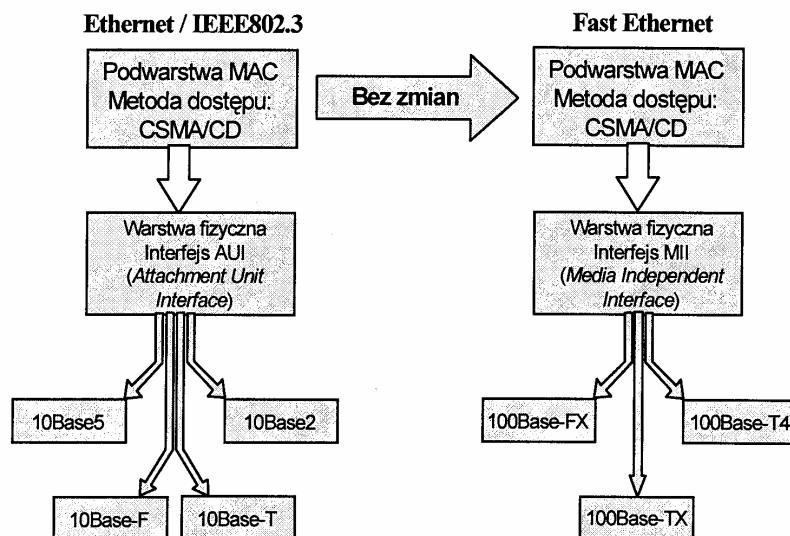
Rys. 4.49. Ilustracja stosowania hubów w standardzie 100VG-AnyLAN

#### 4.2.6.2 Fast Ethernet

Rozwiązań Fast Ethernet, czyli standard szybkiej sieci lokalnej opartej na technologii Ethernetu zostało opracowany przez firmy: Grand Junction Networks, 3Com, SynOptics, Intel i kilku innych producentów sprzętu i oprogramowania komputerowego. Standard ten jest rozwijany przez Komitet 3 IEEE 802, który w połowie czerwca 1995 roku zatwierdził go jako rozszerzenie standardu 802.3 (pod nazwą IEEE 802.3u). Został on również zaakceptowany przez ISO jako ISO 8802.3u.

Fast Ethernet, znany też pod nazwą 100Base-T, stanowi modyfikację dotychczas funkcjonujących odmian standardu Ethernet, zwiększącą szybkość przesyłu danych do 100 Mb/s. Jest to technologia bardzo podobna do 10Base-T. Zachowana została metoda zarządzania dostępem - CSMA/CD, co przy 10-cio krotnym zwiększeniu szybkości transmisji spowodowało dość znaczne ograniczenie dopuszczalnej rozpiętości sieci. Nie uległy natomiast zmianie format ramek, ich długość oraz metoda kontroli błędów. Zmieniły się jednakże techniki kodowania sygnałów jak i rodzaje mediów, z którymi standard współpracuje. Założono jednak, że zmiany te nie mogą wykluczać możliwości współpracy obu rodzajów Ethernetu. Od urządzeń Fast Ethernetowych, w celu łagodnego przejścia do nowszej technologii, wymaga się więc możliwości współpracy z innymi urządzeniami Ethernetowymi, a do dodatkowych funkcji, w porównaniu z 10Base-T, realizowanych przez hub Fast Ethernetowy należy proces Auto-Negocjacji (ang. *Auto-Negotiation*) umożliwiający automatyczne rozpoznanie trybu pracy urządzeń podłączonych do huba.

Porównanie pomiędzy Ethernetem i Fast Ethernetem zostało przedstawione na rysunku 4.50.



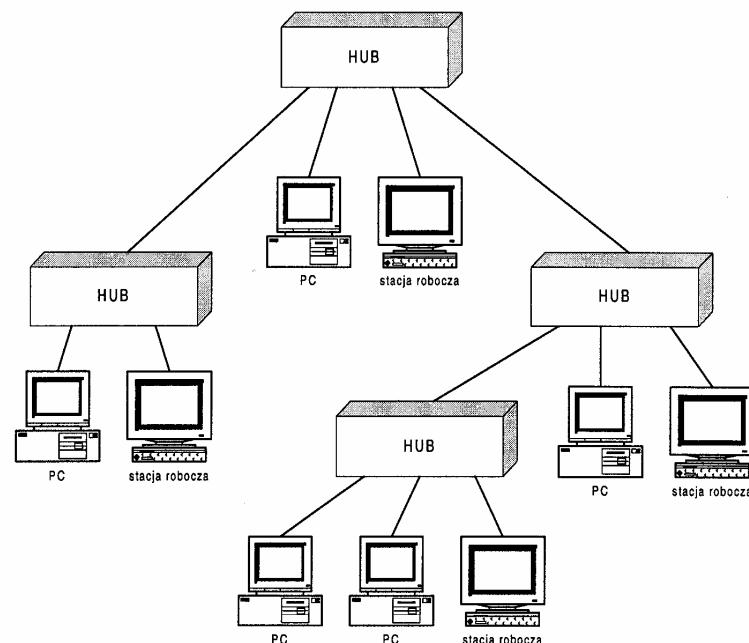
Rys. 4.50. Porównanie standardów Ethernet i Fast Ethernet

Nowy standard, 100Base-T, przewiduje możliwość współpracy z trzema rodzajami medium transmisyjnego. Poszczególne wersje Fast Ethernet to:

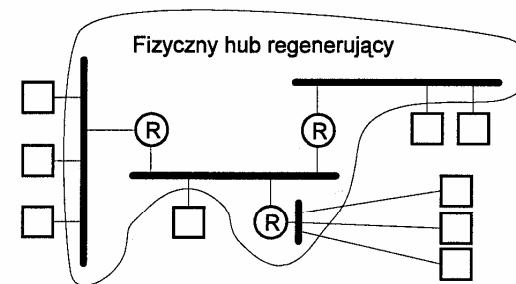
- system 100Base-TX używający dwóch par skrętek typu UTP (ang. *Unshielded Twisted Pair*) i STP (ang. *Shielded Twisted Pair*) kategorii 5 (standard EIA 568 Category 5) o maksymalnej długości segmentu nie przekraczającej 100 metrów; rozwiązań 100Base-TX oparte jest na specyfikacji ANSI (ang. *American National Standard Institute*): X3T9.5, i wykorzystuje te same układy dostępu do kanału fizycznego co w standardach FDDI i CDDI;
- system 100Base-T4 wykorzystujący cztery pary skrętek kategorii 3, 4 lub 5 o maksymalnej długości segmentu wynoszącej 100 metrów;
- system 100Base-FX opierający się na pojedynczej nitce światłowodowej wielomodowej o średnicy rdzenia 62.5 µm i średnicy płaszcza 125 µm z maksymalną długością segmentu wynoszącą 412 metrów.

#### 4.2.6.2.1 Topologia sieci ethernetowej

W przypadku topologii sieci Ethernet należy rozróżnić pojęcia topologii fizycznej (tzn. rozmieszczenia przestrzennego kabli) od topologii logicznej. W sieci Fast Ethernet stosowana jest topologia fizyczna typu gwiazdy, w której, tak jak w sieciach 10Base-T, wszystkie przewody biegą, zgodnie z ilustracją zamieszczaną na rysunku 4.51, do centralnego huba.



Rys. 4.51. Topologia sieci Fast Ethernet



Rys. 4.52. Przykładowa topologia logiczna

Osią logiczną każdej sieci ethernetowej jest magistrala, do której dołączone są wszystkie stacje. W przypadku klasycznej sieci ethernetowej logiczna magistrala odpowiada magistrali fizycznej. Kilka segmentów sieci (formalnie segment zdefiniowany jest jako połączenie punkt-punkt łączące dwa i tylko dwa interfejsy MDI (ang. *Media Dependent Interface*); oznacza to, że tworząc sieć liczącą kilka

stacji musimy użyć huba) może być połączonych razem za pomocą tzw. repeaterów w celu utworzenia większej i bardziej elastycznej sieci. Istotne jest, aby każdy segment „miał dwa końce”, gdyż segmenty nie mogą tworzyć pętli. Przykładową konfigurację sieci ethernetowej przedstawia rysunek 4.52. Konfiguracja taka może być zrealizowana w klasycznym etherencie (tzn. z fizycznie istniejącą magistralą). W rozwiązańach 10BASE-T oraz 100BASE-T logiczna magistrala i repeater przyjmują fizycznie postać tzw. regenerującego huba (ang. *repeating hub*), co zmienia topologię z magistralowej na gwiazdową.

Podstawową wadą technologii Fast Ethernet (podobnie jak standardowego Ethernetu) jest to, że topologia sieci nie może być zbyt rozbudowana. Ograniczenie dotyczy maksymalnej odległości między dwiema skrajnymi stacjami w sieci, nie mogącą, w wypadku stosowania kabla UTP, przekroczyć 200 metrów. Odległość ta jest limitowana przez minimalną długość ramki i szybkość propagacji sygnałów w medium oraz opóźnienia wnoszone przez urządzenia sieciowe, w szczególności huby.

Istnieją dwa główne rodzaje hubów, tzw. huby regenerujące (ang. *repeating hubs*) i huby przełączające (ang. *switching hubs*). Pierwszy rodzaj hubów służy do łączenia poszczególnych segmentów sieci, zaś drugi rodzaj - do łączenia odrębnych sieci LAN.

Fast Ethernet wykorzystuje dwie klasy hubów regenerujących nazywanych repeaterami: I i II klasy (w standardzie klasy te oznaczone są odpowiednio rzymską cyfrą I lub II położoną wewnątrz okręgu).

Repeater klasy I może być wykorzystany do łączenia segmentów zbudowanych w oparciu o różne media (np. do łączenia TX z T4). Musi on przy tym sam przetwarzanie sygnały odebrane z jednego segmentu do postaci cyfrowej akceptowanej w drugim segmencie. Proces translacji wykonywany w repeaterze klasy I (realizowany zawsze, bez względu na to czy jest on potrzebny, czy też nie, gdy repeater łączy takie same segmenty) wprowadza tak duże opóźnienie, że tylko jeden repeater klasy I może być użyty w pojedynczej domenie kolizyjnej, jeżeli wykorzystywana jest maksymalna długość kabla.

Repeater klasy II może współpracować tylko z tym samym rodzajem medium. Nie dokonuje on przetwarzania odbieranych sygnałów do określonej postaci cyfrowej, a jedynie powiela odebrane sygnały, regenerując je i przesyłając na inne porty. Dzięki temu wprowadza mniejsze opóźnienia. Oznacza to w praktyce, że przy wykorzystywaniu maksymalnej długości kabla można użyć dwa repeaterów klasy II w jednej domenie kolizyjnej.

Maksymalne rozpiętości domen kolizyjnych przedstawiono w tabeli 4.4. Podane w tej tabeli maksymalne odległości między urządzeniami sieciowymi wynikają z protokołarnego ograniczenia narzuconego na minimalną długość ramki, przyjętego w celu wykrycia kolizji (512 bitów, których czas transmisji jest równy 5120 ns), i opóźnień wprowadzanych przez poszczególne urządzenia sieciowe. Przyjmuje się, że poszczególne urządzenia sieciowe lub odcinki mediów wnoszą następujące opóźnienia:

- repeater klasy I - do 1400 ns,
- repeater klasy II ze wszystkimi portami typu TX/FX - do 920 ns,
- repeater klasy II z portami typu T4 - do 670 ns,
- dwie stacje (DTE) dołączone do medium TX/FX - do 1000 ns,
- 412 metrów światłowodu - do 4120 ns,
- 100 metrów kabla kategorii 3 - do 1140 ns,
- 100 metrów kabla kategorii 5 - do 1112 ns.

Tabela 4.4. Maksymalne rozpiętości domen kolizyjnych

Typ regeneratora	Przewody miedziane	Światłowody (długość w metrach)	Przewody miedziane i światłowody (T4 i FX)	Przewody miedziane i światłowody (długość w metrach)
Pojedynczy segment DTE-DTE	100	412	N/A	N/A
Regenerator klasy I	200	272	231	260.8
Regenerator klasy II	200	320	N/A	308.8
Dwa regeneratory klasy II	206	228	N/A	216.2

N/A - nie zdefiniowane

Predkość propagacji sygnałów silnie zależy od typu medium. Dla światłowodów można ją oszacować jako  $v = c/n = 0.2 \text{ m/ns}$ , gdzie  $c = 3 \cdot 10^8 \text{ m/s}$  (predkość rozchodzenia się światła w próżni), a  $n$  - współczynnik załamania światła (typowo  $n=1.5$ ). Przykładowe predkości (w stosunku do  $c$ ) propagacji sygnału w kablach różnych producentów przedstawiono w tabeli 4.5.

Tabela 4.5. Przykładowe znormalizowane predkości propagacji sygnału w kablach wyrażone w % (dla skrętki niekranowanej 24AWG)

Nazwa	Kategoria	v/c [%]
AT&T1010	3	67%
AT&T1041	4	70%
AT&T1061	5	70%
AT&T2010	3	70%
AT&T2041	4	75%
AT&T2061	5	75%
Belden1229A	3	69%
Belden1455A	4	72%
Belden1583A	5	72%
Belden1245A2	3	69%
Belden1457A	4	75%
Belden1585A	5	75%

Zatem np. przy połączeniu dwóch stacji DTE za pomocą medium światłowodowego, podwojona odległość między nimi może być wyznaczona jako iloczyn {minimalnego czasu transmisji ramki (5120 ns) pomniejszonego o opóźnienie wnoszone przez urządzenia sieciowe DTE (1000 ns)} oraz prędkości propagacji sygnałów w światłowodzie (0.2 m/ns). Obliczona w ten sposób droga wynosi 824 m. Tym samym maksymalna odległość między dwiema stacjami DTE jest równa 824 m:  $2 = 412$  m. Jeżeli na odcinku łączącym dwie stacje DTE zastosujemy repeater klasy I (wprowadzający opóźnienie 1400 ns), to podobnie jak w opisany powyżej przypadku, podwojona odległość między stacjami może być wyznaczona jako iloczyn (minimalnego czasu transmisji ramki pomniejszonego o sumę opóźnień wnoszonych przez urządzenia sieciowe DTE i repeater klasy I) oraz prędkości propagacji sygnałów w światłowodzie. Tym samym maksymalna odległość między dwiema stacjami DTE jest równa 272 m ( $\{[5120 \text{ ns} - (1000 \text{ ns} + 1400 \text{ ns})] * 0.2 \text{ m/ns}\} : 2 = 272$ ).

Poza różnymi szybkościami pracy, do istotnych różnic pomiędzy 10Base-T i 100Base-T należy też zaliczyć zmianę metody kodowania, zastosowaną w celu lepszego wykorzystania przepustowości łącza. W przypadku 10Base-T używa się kodu Manchester. Dla szybkości przesyłania informacji, wynoszącej 10 Mb/s, mamy wówczas szybkość modulacji 20 MBodów. Pozwala to na zaledwie 50% wykorzystywanie całkowitej przepustowości łącza. W standardzie 100Base-T stosuje się kodowanie 4B/5B pozwalające na 80% wykorzystanie przepustowości łącza.

#### 4.2.6.2.2 Auto-Negocjacja

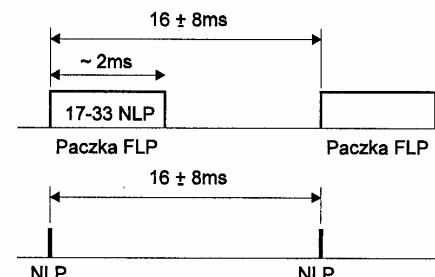
W standardzie Fast Ethernet interfejsy sieciowe mogą pracować w wielu trybach, w zależności od rodzaju wykorzystywanego w sieci medium. Celem realizacji procedur Auto-Negocjacji jest umożliwienie współpracy różnych urządzeń w trybie o „najwyższym”, akceptowanym przez wszystkie urządzenia, priorytety. Przypisanie priorytetów medium a tym samym trybom pracy, od najwyższego do najniższego, przedstawiono w tabeli 4.6.

Tabela 4.6. Przyporządkowanie priorytetów protokołu Autonegoacji różnym typom okablowania sieci

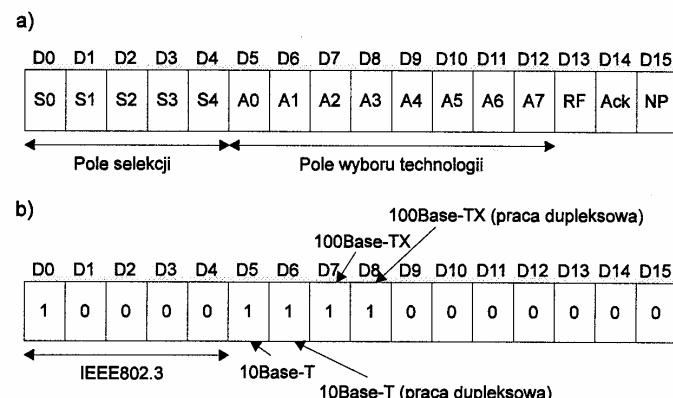
A:	100BASE-TX Full Duplex
B:	100BASE-T4
C:	100BASE-TX
D:	10BASE-T Full Duplex
E:	10BASE-T

Proces Auto-Negocjacji generuje i wykorzystuje sygnały zwane *Fast Link Pulse* (ang. FLP). Sygnały te tworzą paczki (ang. burst) składające się z 33 impulsów, z których 16 o numerach parzystych przenosi informację, zaś 17 o numerach

nieparzystych wykorzystywanych jest do celów synchronizacji. Odstęp czasu pomiędzy poszczególnymi impulsami wynosi  $62.5\mu\text{s} +/- 7\mu\text{s}$ , a pomiędzy całymi słowami - 16ms +/- 8ms (ilustruje to rysunek 4.53). Brak impulsu informacyjnego pomiędzy kolejnymi impulsami synchronizacji (w paczce) oznacza logiczne zero, a jego pojawienie się - logiczną jedynkę. Sygnały FLP są zmodyfikowaną wersją sygnałów NLP (ang. Normal Link Pulse) stosowanych w 10Base-T. Tak więc urządzenia standardu 10BASE-T nie mają trudności z nawiązaniem współpracy z urządzeniami Fast Ethernetu. System Auto-Negocjacji zezwala również na „ręczne” wymuszenie wymaganego trybu pracy na wybranym porcie huba.



Rys. 4.53. Długość trwania „słów” FLN i NLP



Rys. 4.54. Struktura ramki Auto Negocjacji: a) wykorzystanie bitów informacyjnych, b) przykładowe słowo kodowe

Na rysunku 4.54 przedstawiono strukturę ramek protokolarnych (będących wspomnianymi powyżej ciągami 16-stu impulsów o numerach parzystych) wykorzystanych w procesie Auto-Negocjacji. Pole selekcji (ang. Selector Field) określa rodzaj standardu i obecnie może przyjmować tylko wartości 10000 dla IEEE 802.3 oraz 0100 dla IEEE 802.9 (standard Iso Ethernet). Inne kombinacje

są na razie zastrzeżone do przyszłego wykorzystania. Pole wyboru technologii (ang. *Technology Ability Field*) zawiera informacje o możliwości współpracy z poszczególnymi trybami.

Ustawienie bitu Ai dla i=0,1,...,7 oznacza:

- A0 - 10BASE-T
- A1 - 10BASE-T Full Duplex
- A2 - 100BASE-TX
- A3 - 100BASE-TX Full Duplex
- A4 - 100BASE-T4

Bit A5, A6 i A7 zarezerwowane są dla przyszłych technologii.

Bit RF (ang. *Remote Fault*) informuje o błędzie w oddalonej stacji. Bit Ack (ang. *Acknowledge*) ustawiany jest przez stację po wykryciu trzech pełnych słów protokołu (od swojego „rozmówcy”) zaś bit NP (ang. *Next Page*) oznacza, że stacja chce przejść do następnego etapu negocjacji.

Proces negocjacji obejmuje:

- wymianę, przez obu partnerów, słów FLP bez ustawionego bitu Ack,
- ustawienie bitu Ack przez stację, która wykryła trzy pełne słowa FLP od partnera,
- nadanie od 6 do 8 słów i uznanie przez stację procesu Auto-Negocjacji jako przeprowadzonego z sukcesem, po wykryciu przez stację kolejnych trzech pełnych słów FLP z ustawionym bitem Ack; w przeciwnym wypadku przejście stacji do następnego etapu negocjacji.

Jeśli urządzenia nie uzgodnią wspólnego trybu, to połączenie nie zostanie ustalone.

Protokół Auto-Negocjacji umożliwia również realizację trybu Full Duplex, który na obecnym poziomie standaryzacji Auto-Negocjacji jest osiągalny dla 100BASE-TX oraz 10BASE-T. Tryb Full Duplex może być zrealizowany tylko między dwoma urządzeniami. Nie jest więc współdzielony kanał ani też urządzenia nie muszą nasłuchiwać łączą (nie jest realizowany protokoł dostępu do łączą typu CSMA/CD). Daje to możliwość tworzenia znacznie dłuższych połączeń; w przypadku łączą światłowodowego (bez Auto-Negocjacji) są to typowo 2 km (zasięg ten jest ograniczony tylko tłumieniem w medium).

W przypadku, gdy protokół Auto-Negocjacji jest zaimplementowany tylko w jednym z urządzeń, to zostaje to wykryte i obsłużone za pomocą mechanizmu tzw. równoległego wykrywania (ang. *Parallel Detection*).

Pomimo, że protokół Auto-Negocjacji umożliwia pracę w różnych trybach to jednak wszystkie porty regenerującego huba muszą pracować z tą samą szybkością. Nie jest więc możliwe stworzenie sieci ethernetowej pracującej jedno-

cześnie z szybkością 10 Mb/s i 100 Mb/s. Oznacza to, że jeden hub obsługiwany może wyłącznie urządzenia pracujące albo z szybkością 100 Mb/s albo też 10 Mb/s. Ograniczenie to nie występuje w przypadku huba przełączającego (ang. *switching hub*).

#### 4.2.6.3 Porównanie technologii 100VG-AnyLAN i Fast Ethernet oraz innych rozwiązań sieci lokalnych

Porównując obie technologie, tj. 100VG-AnyLAN i Fast Ethernet wydaje się, że nieco elastyczniejszą z nich jest 100VG-AnyLAN z uwagi na lepszy protokół dostępu oraz lepsze mechanizmy bezpieczeństwa. Przeglądając się technologii 100Base-T (Fast Ethernet), dochodzimy do wniosku, że konstruktorzy uczynili wszystko, aby była ona maksymalnie podobna do technologii stosowanej w sieciach standardu 10Base-T. Spowodowało to przejęcie nie tylko zalet, ale i wszystkich wad tej technologii (patrz rozdział 4.2.1), w szczególności możliwość występowania kolizji.

Rozważając możliwości przejścia z technologii 10 Mb/s na technologię 100 Mb/s (Fast Ethernet bądź 100VG-AnyLAN) warto zwrócić uwagę na kilka spraw:

- Oba standardy wymagają wymiany kart sieciowych, przy czym 100VG-AnyLAN jest bardziej kompatybilny z okablowaniem 10Base-T.
- Producenci oferują karty 100Base-X, zdolne do pracy z Ethernetem 10 Mb/s, co ułatwia przejście na nowy standard.
- 100Base-T wymaga kabli kategorii 5 (komputerowych), podczas gdy 100VG-AnyLAN - czteroparowej skrętki telefonicznej.

Krótkie porównanie pozostałych parametrów i cech funkcjonalnych protokołów Fast Ethernet, 100VG-AnyLAN i omawianych wcześniej standardów serii IEEE 802 zamieszczono w tabelach 4.7 i 4.8.

Tabela 4.7. Porównanie parametrów standardowych rozwiązań lokalnych sieci komputerowych

	IEEE 802.3 Ethernet	IEEE 802.3 Fast Ethernet	IEEE 802.4 Token Bus	IEEE 802.5 Token Ring	IEEE 802.12 100VG-AnyLAN
Długość ramki [ bajt]	1518/1526	1518	8191	4500-4 Mb/s 8000-16 Mb/s	1518-802.3 8000-802.5
Szybkość transmisji [Mb/s]	1 - 20	100 - 200	1, 5, 10, 20	4, 16	100
Priorytety	brak	brak	4 poziomy	8 poziomów	2 poziomy
Kolejność przesyłanych bitów	od najbardziej znaczącego do najmniej znaczącego	od najbardziej znaczącego do najmniej znaczącego	od najbardziej znaczącego do najmniej znaczącego	od najmniej znaczącego do najbardziej znaczącego	w zależności od współpracy ze standardem 802.3 bądź 802.5

Tabela 4.8. Zestawianie najważniejszych parametrów i cech standardów IEEE 802.3, IEEE 802.3 Fast Ethernet i 100VG-AnyLAN

	10Base - T	100VG - AnyLAN	100Base - T
<b>Długość sieci</b>	2500m	2500m	412m
<b>Łączenie kaskadowe wielopoziomowe</b>	Tak ; 3 - poziomy	Tak ; 3 - poziomy hubów	2 huby
<b>Maksymalna długość kabla od hub'a do węzła:</b>			
Skrętka ( UTP ) kat. 3,4	100m	100m	100m
Skrętka (UTP ) kat. 5	150m	200m	100m
25- parowa skrętka (UTP)	Tak	Tak	Nie
Skrętka ekran. (STP)	100m	100m	100m
Światłowód	2000m	2000m	412m
<b>Wykorzystanie przepustowości dla długości kabla :</b>			
100 m	80 % (teoretycznie)	95 %	80 % (teoretycznie)
2500 m	80 %	80 %	brak
<b>Kompatybilność z ramką 802.3/Ethernet</b>	Tak	Tak	Tak
<b>Kompatybilność z ramką 802.5 Token-Ring</b>	Nie	Tak	Nie
<b>Dostęp do medium</b>	CSMA/CD	Demand Priority	CSMA/CD

Różnice pomiędzy poszczególnymi standardami powodują, że przy współpracy tych sieci należy wykonywać szereg czynności „dostosowawczych” już na poziomie ich najniższych warstw. Zagadnienia te będą przedmiotem naszego zainteresowania w rozdziale 9.

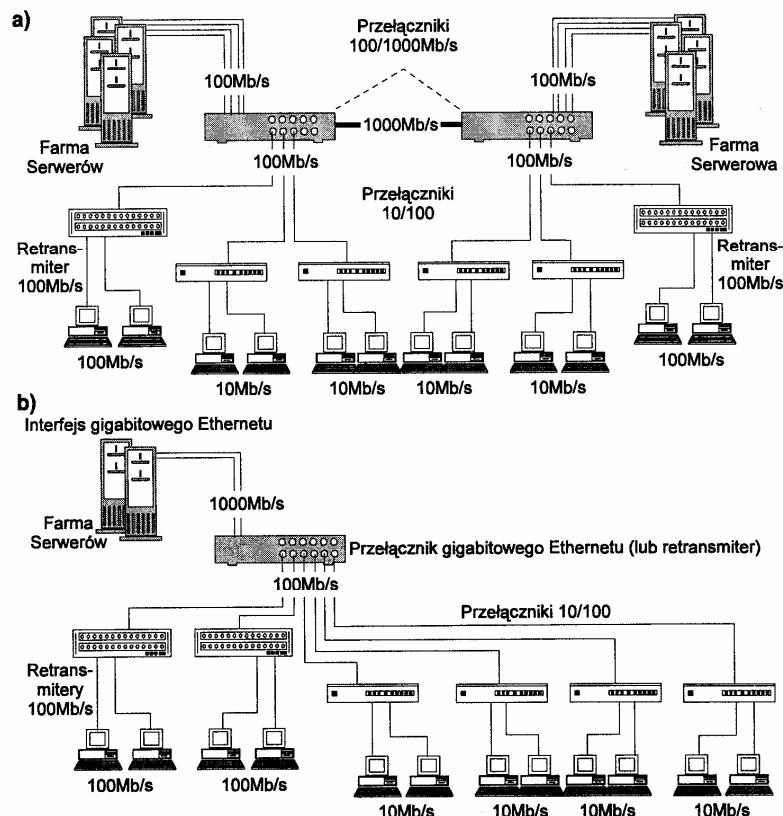
#### 4.2.6.4 Gigabitowy Ethernet

Dalszym rozwinięciem standardów sieciowych opartych na protokole Ethernetu jest Gigabitowy Ethernet. Oferuje on przekaz danych z szybkością około 1 Gb/s, a jednocześnie zapewnia możliwość wykorzystania istniejącej infrastruktury sieciowej, zainstalowanej z myślą o zwykłym Etherencie bądź Fast Etherencie.

Gigabitowy Ethernet umożliwia pracę pełnodupleksową na łączach pomiędzy specjalizowanymi przełącznikami 100/1000 Mb/s i pomiędzy przełącznikami a stacjami końcowymi (serwerami) oraz tryb pracy półdupleksowej w przypadku łączy ze współdzielonym medium, z wykorzystaniem hubów i metody dostępu CSMA/CD.

#### 4.2.6 Szybkie sieci LAN

Standard Gigabitowego Ethernetu wykorzystuje głównie skrętkę nieekranowaną (UTP) 5 kategorii. Dzięki temu, że Gigabitowy Ethernet pozwala na wykorzystanie istniejącej i sprawdzonej technologii, można oczekiwać na jego szybkie wprowadzenie do powszechnego użytku. Wysiłki komitetu normalizacyjnego IEEE 802.3z skupiają się na badaniu i opracowywaniu zaleceń odnośnie kanałów światłowodowych i innych elementów szybkiej sieci LAN. Stosowane obecnie techniki kodowania (8B/10B) i dekodowania pozwalały na uzyskanie szybkości transmisji 1.063 Gb/s. Oczekuje się, że już wkrótce możliwy będzie przekaz z szybkością 1.250 Gb/s. Na dłuższych odcinkach (do 2 km) stosowane będą światłowody jednomodowe, natomiast na odcinkach do 550 m zastosowanie znajdą światłowody wielomodowe. Przykładowe topologie sieci LAN wykorzystujące technologię Giga Ethernetu ukazuje rysunek 4.55.



Rys. 4.55. Przykładowe konfiguracje sieci Giga Ethernet

#### 4.2.7 IsoEthernet IEEE 802.9 - multimedialny LAN

Wśród użytkowników sieci LAN coraz większe zainteresowanie wzbudzają usługi multimedialne. Realizacja tego typu usług wymaga jednakże systemów sieciowych, zdolnych przekazywać informacje ze stałą szybkością (systemy multimedialne są z natury rzeczy systemami czasu rzeczywistego). Większość współczesnych sieci LAN, a w szczególności sieci Ethernet (IEEE 802.3), to sieci pakietowe, których możliwości nie są wystarczające do realizacji np. wideokonferencji - tj. usług coraz bardziej popularnej, wymagającej jednakże transmisji synchronicznej. Z uwagi na to, że sieci lokalne są instalowane w biurach, bankach, czy też instytucjach naukowo-badawczych, rozsądnym rozwiązańem może być wykorzystanie tego samego medium do przesyłania zarówno obsługiwanych w trybie asynchronicznym danych, jak i innych informacji, np. lokalnych i pozalokalnych rozmów telefonicznych. Opracowany ostatnio standard IEEE 802.9, określany też mianem IsoEthernetu, rozwiązuje te problemy, pozwalaając na stosunkowo proste pogodzenie wymagań przesyłania informacji synchronicznych i asynchronicznych. W IsoEthercie zintegrowano rozwiązanie Ethernetu 10Base-T z usługami izochronicznymi, oferowanymi przez ISDN. Sama technika ISDN nie jest wystarczającym rozwiązaniem komunikacyjnym, gdyż pojedynczy kanał ISDN ma przepustowość jedynie 64 kB/s, i nawet zastosowanie szerokopasmowych usług ISDN w kanałach pierwotnogrupowych daje szybkość transmisji nie większą niż 2 Mb/s. Dla większości typowych zastosowań sieci LAN jest to szybkość zbyt mała. Z kolei rozwiązanie Ethernet, z szybkością 10 Mb/s, nie pozwala na transmisję synchroniczną. W przeciwieństwie do IEEE 802.3, sieci standardu IEEE 802.9 pozwalają realizować w jednym medium oba typy połączeń - z komutacją pakietów (Ethernet) i komutacją kanałów (ISDN). Dwoistość ta powoduje, że sieć IsoEthernet jest siecią hybrydową (a nie jak typowy Ethernet - siecią homogeniczną).

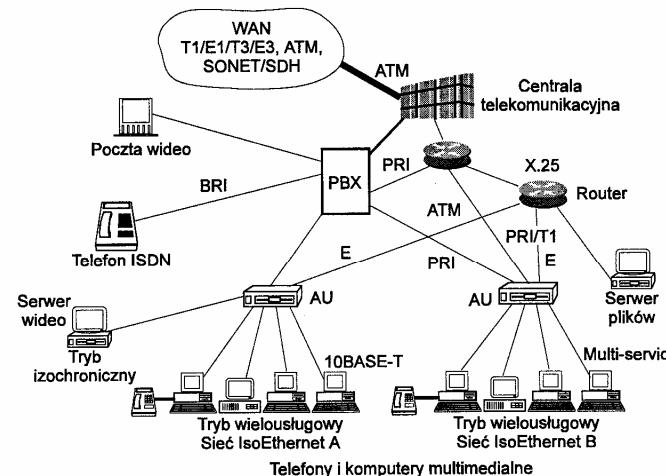
##### 4.2.7.1 Topologia sieci

IsoEthernet jest rozwiązaniem sieci lokalnej, które zapewnia realizację usług izochronicznych, synchronicznych i asynchronicznych oraz może bezpośrednio współpracować z innymi standardami sieciowymi. Prowadzone są też prace nad realizacją usług w trybie komutacji komórek.

Podobnie jak 10Base-T, IsoEthernet jest siecią o topologii gwiazdy, gdzie urządzenia użytkowników podłączone są do układu dostępu (ang. AU - Access Unit - przełącznik typu hub/centrala PBX - *Private Branch Exchange*).

Przykładową topografię sieci IEEE 802.9 obrazuje rysunek 4.56.

Do poszczególnych segmentów sieci IsoEthernet dołączane są komputery osobiste, stacje robocze oraz komputery multimedialne. Do ich przyłączenia do układu AU (specjalizowanego huba) wykorzystuje się dwie pary popularnej skrętki nie-ekranowanej UTP, klasy co najmniej 3, o długości nie przekraczającej 100 m. Komunikacja pomiędzy poszczególnymi jednostkami sieci odbywa się za pośrednictwem sieci rozlegiej.



Rys. 4.56. Przykładowa topologia sieci IsoEthernet

##### 4.2.7.2 Układy dostępu AU

Podstawową funkcją układu dostępu AU (zwykle jest to hub lub centrala PBX) jest zapewnienie łączności pomiędzy urządzeniami, w tym - urządzeniami multimedialnymi IsoEthernetu i/lub typowymi urządzeniami sieci 10Base-T.

Zadania realizowane przez AU obejmują też:

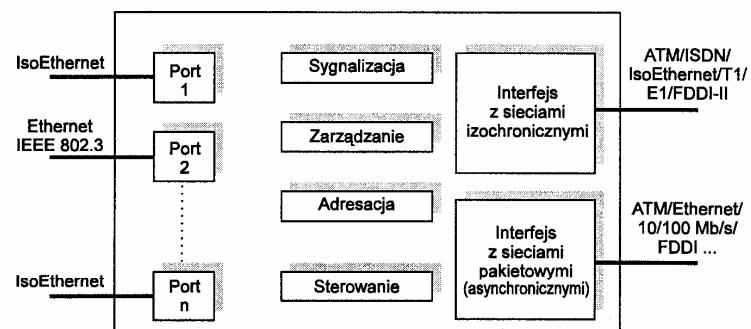
- przenoszenie informacji w postaci ramek Ethernetu,
- komamację i multipleksację pakietów,
- nadzorowanie procesów zarządzania, sygnalizacji i adresacji w sieci.

Ponadto układ AU pełni funkcje :

- retransmitera ramek do/z różnych portów, tworzących wspólną domenę kolizyjną,
- mostu i przełącznika ramek w sieci (w zależności od potrzeb),
- interfejsu z asynchronicznymi sieciami szkieletowymi typu ATM, FDDI lub 100Base-T.

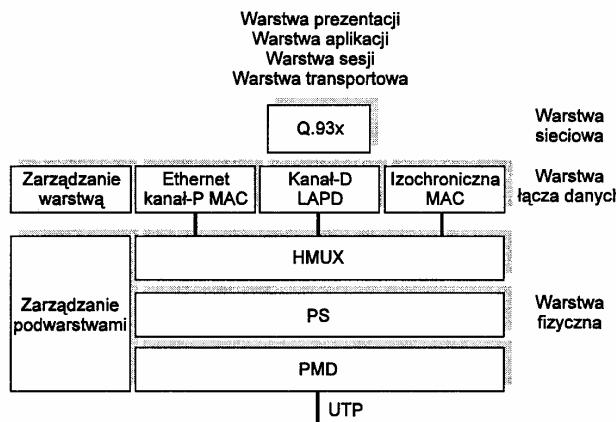
Struktura blokowa układu dostępu przedstawiona jest na rysunku 4.57.

Układ dostępu posiada interfejs komutacji i multipleksacji izochronicznej, który umożliwia dynamiczną komutację kanałów (tzw. kanałów typu C). Interfejs ten może być wykorzystany do współpracy z innymi sieciami izochronicznymi (ISDN, E1/T1, FDDI-II, SONET) lub sieciami realizującymi usługi ze stałą szybkością bitową (ang. CBR - *Constant Bit Rate*), np. z siecią ATM. Stacje końcowe oraz porty AU są zarządzane przez moduł zarządzający. Moduł adresujący odpowiada za właściwe adresowanie informacji przepływających przez sieć IsoEthernet.



Rys. 4.57. Model układu dostępu AU

#### 4.2.7.3 Architektura sieci IsoEthernet

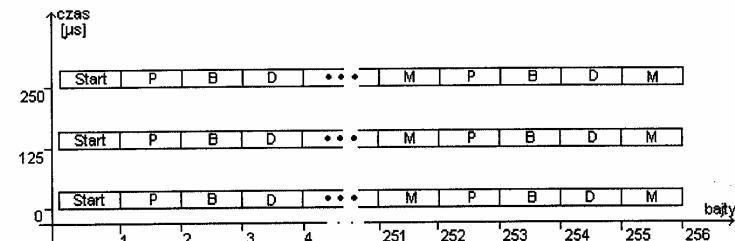


Rys. 4.58. Architektura sieci IsoEthernet w odniesieniu do modelu ISO-OSI

Technologia sieci IsoEthernet wykorzystuje dwie pary popularnej nieekranowanej skrętki UTP, klasy co najmniej 3, o długości nie przekraczającej 100 m. Model warstwowy standardu IEEE 802.9 przedstawiony jest na rysunku 4.58.

#### Warstwa łączna danych

W standardzie IEEE 802.9 warstwa łączna danych zapewnia realizację usług uwierunkowanych czasowo. Jest to możliwe dzięki wykorzystaniu metody zwielokrotnienia czasowego medium i multipleksacji kanałów (ang. TDM - *Time Division Multiplexing*), podobnie jak w systemie PCM. Polega to na tym, że co 125 μs, czyli z częstotliwością 8 kHz - tak, jak w ISDN i cyfrowej telefonii publicznej - generowane są, przez układy dostępu, ramki czasowe o długości 256 bajtów. Poszczególne szczeliny czasowe tych ramek tworzą 256 podkanałów logicznych.



Rys. 4.59. Multipleksacja kanałów w ramce TDM sieci IsoEthernet

Rysunek 4.59 pokazuje ideę multipleksacji kanałów w ramce TDM sieci IsoEthernet.

W warstwie łączna danych wyodrębniono i zdefiniowano 5 typów kanałów, wykorzystujących ramkę TDM do realizacji odpowiednich usług. Są to:

- kanał P - w zależności od konfiguracji ustalonej na etapie tzw. algorytmu sygnalizacyjnego autonegoacji, jest kanałem półdupleksem albo dupleksem o przepływności 10 Mb/s, przenoszącym informacje asynchroniczne Ethernetu zgodnie z protokołem CSMA/CD,
- kanał C - jest kanałem dupleksem, wykorzystywanym do realizacji usług wymagających komutacji kanałów. W zależności od konfiguracji może on pracować w jednym z dwóch trybów :
  - izochronicznym - obsługuje wtedy kanały o przepustowości od 64 kb/s do 15,872 Mb/s (pojedynczy kanał posiada przepustowość 64 kb/s i odpowiada kanałowi B w ISDN, zgodnie z ilustracją na rysunku 4), lub
  - wielousługowym - dostępne jest wtedy pasmo 6,144 Mb/s,
- kanał D - jest kanałem dupleksem o przepustowości 64 kb/s, pełniącym rolę kanału pomocniczego przy realizacji połączeń w kanale C. Z jego udziałem dokonywane jest zestawianie i rozłączanie połączeń, a także utrzymanie i zabezpieczenie transmisji (połączenia typu punkt-wielopunkt, wielopunkt-wielopunkt). Umożliwia on również (podobnie jak w ISDN) przesyłanie pakietów zgodnie z protokołem X.25,
- kanał M - jest kanałem dupleksem o przepustowości 96 kb/s. Pełni on rolę kanału pomocniczego, służącego do przekazywania informacji utrzymywanych i synchronizacyjnych (8 kb/s) sieci,
- kanał synchronizacji ramki - jest to kanał o przepustowości 64 kb/s. Jego zadaniem jest przenoszenie informacji o początku nowej ramki czasowej co 125 μs (kanał ten odpowiada pierwszej szczerelinie czasowej ramki).

Kanał P wykorzystuje mechanizm CSMA/CD (tak, jak w typowym rozwiązaniu IEEE 802.3). Tym samym IsoEthernet jest zgodny ze zwykłym Ethernetem 10Base-T. Z kolei kanały synchroniczne C i D sieci IsoEthernet mogą być wykorzystane do realizacji usług ISDN.

W warstwie łącza danych wyróżniono również podwarstwę zarządzającą poszczególnymi blokami funkcjonalnymi (por. rysunek 4.58).

#### 4.2.7.4 Tryby pracy IsoEthernetu

Standard IEEE 802.9 definiuje trzy tryby, w których mogą pracować urządzenia sieci IsoEthernet. Są to :

- tryb wielousługowy,
- tryb izochroniczny,
- tryb standardowy 10Base-T.

Tryby te są ustalane automatycznie przez hub - układ dostępu AU - w chwili włączenia zasilania do urządzenia użytkownika. Dzięki temu IsoEthernet zapewnia współpracę, w jednej sieci, urządzeń standardu IEEE 802.3 z urządzeniami wymagającymi transmisji synchronicznej. Automatyczna konfiguracja trybów pracy jest możliwa dzięki algorytmom sygnalizacyjnym autonegoacji, które potrafią wykryć typ urządzenia końcowego.

Poszczególne tryby realizują następujące usługi:

- tryb wielousługowy (ang. *Multi-Service Mode*) - umożliwia obsługę w jednym medium sieci asynchronicznej 10Base-T i synchronicznych kanałów komutowanych:
  1. kanał P o przepustowości 10 Mb/s (standard IEEE 802.3),
  2. kanał C o przepustowości 6,144 Mb/s, składający się z 96 kanałów ISDN 64 kb/s,
  3. kanał D o przepustowości 64 kb/s,
  4. kanał M o przepustowości 96 kb/s,
  5. kanał synchronizacji ramki o przepustowości 64 kb/s;
- tryb izochroniczny (ang. *Isochronous Mode*) - w trybie tym wszystkie usługi oparte są na komutacji kanałów. Maksymalna szybkość transmisji w tym trybie wynosi 15,872 Mb/s, a transmisje realizowane są synchronicznie. Strumień informacji jest kodowany metodą 4B/5B i przekształcany do formatu NRZI, a następnie transmitowany przez medium. W trybie izochronicznym nie występuje kanał P (w którym normalnie realizowany jest protokół CSMA/CD),
- tryb 10Base-T - tryb ten jest zgodny ze standardem IEEE 802.3 - transmisja asynchroniczna odbywa się z szybkością do 10 Mb/s; informacje w linii transmisyjnej kodowane są kodem Manchester. W trybie tym występuje tylko kanał P pracujący zgodnie z protokołem CSMA/CD.

#### 4.2.7.5 Warstwa fizyczna IsoEthernetu

Zadaniem warstwy fizycznej jest zapewnienie odpowiednich mechanizmów transportowych dla wszystkich kanałów warstwy łącza danych.

Warstwa fizyczna sieci IsoEthernet została wyspecyfikowana w standardzie jako IEEE 802.9a. Dla sieci lokalnych zdefiniowano w niej trzy podwarstwy :

- multipleksacji hybrydowej HMUX (ang. *Hybrid Multiplexing*),
- sygnalizacji PS (ang. *Physical Signalling*) i
- podwarstwę zależną od medium fizycznego PMD (ang. *Physical Medium Dependent*).

Podwarstwy te realizują następujące zadania:

- Podwarstwa HMUX multipleksuje strumienie danych z kanałów P, C i D w jeden strumień i przekazuje zmultipleksowane dane do podwarstwy PS. Dane odbierane z podwarstwy PS poddawane są demultipleksacji.
- Podwarstwa PS dodaje do strumienia danych z podwarstwy HMUX informacje o multipleksacji kanałów, koduje dane kodem 4B/5B (podobnie jak w FDDI) i przekazuje je do podwarstwy PMD. W przeciwnym kierunku tj. przy odbiorze, dane z podwarstwy PMD są dekodowane i przekazywane do podwarstwy HMUX.
- Podwarstwa PMD przekształca dane z podwarstwy wyższej do postaci wymaganej przez medium. Przekształcenia sygnału, podawanego do UTP, dokonuje się za pomocą kodu NRZI (ang. *Non Return to Zero Inverted*). Kod NRZI pozwala na przesyłanie danych z szybkością ponad 16 Mb/s przy taktowaniu sieci zegarem 20 MHz (dla porównania standard IEEE 802.3 pozwala osiągnąć jedynie 10 Mb/s, przy tej samej częstotliwości pracy).

Podobnie jak w warstwie łącza danych wyodrębniono blok zarządzający poszczególnymi podwarstwami.

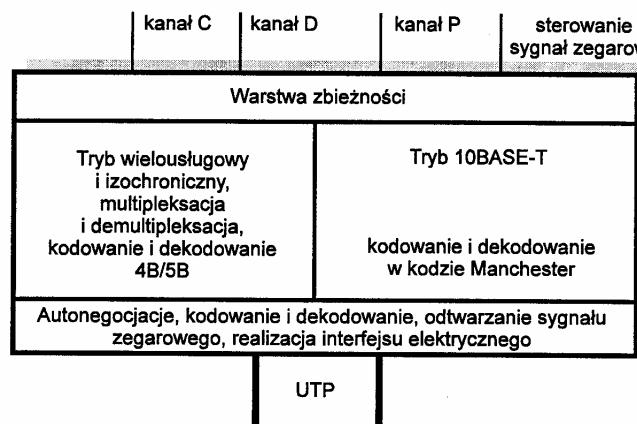
#### 4.2.7.6 Tryby pracy sieci IsoEthernet a warstwa fizyczna

Zgodnie ze specyfikacją IEEE 802.9, sieć IsoEthernet może pracować w trzech trybach - wielousługowym, izochronicznym oraz standardowym 10Base-T.

W trybie wielousługowym i izochronicznym warstwa fizyczna realizuje multipleksację kanałów w szczelinach czasowych TDM. W celu uodpornienia przesyłanych danych na zakłócenia, stosuje się kodowanie ciągów czterobitowych kodem 4B/5B, który następnie przekształca się w kod transmisyjny NRZI. Przy odbiorze najpierw ma miejsce odtwarzanie sygnałów zgodnie z procedurą odwrotną NRZI, a następnie przekształcanie ciągów pięciobitowych na czterobitowe zgodnie z konwersją kodu 4B/5B; dokonywane jest też odtwarzanie sygnałów zegarowych oraz demultipleksowanie kanałów informacyjnych.

W trybie 10Base-T warstwa fizyczna zachowuje się tak samo, jak Ethernet. Informacje kodowane są kodem Manchester. Zapewnia to automatyczną współpracę z urządzeniami IEEE 802.3. Kanały C, D i M są wówczas niedostępne (niedefiniowane).

Poglądowe zestawienie zadań realizowanych przez warstwę fizyczną, w zależności od trybu pracy, przedstawia rysunek 4.60.



Rys. 4.60. Zadania realizowane przez warstwę fizyczną w zależności od trybu pracy sieci IsoEthernet

Algorytm kodowania 4B/5B w połączeniu z NRZI zapewnia aż 80% wykorzystanie przepustowości medium, w porównaniu do kodu Manchester, który wykorzystuje jedynie 50% przepustowości. Zarówno 10Base-T, jak i IsoEthernet używają 20 MHz sygnałów zegarowych, jednak IsoEthernet osiąga przepustowość użytkową 16,384 Mb/s, podczas gdy 10Base-T jedynie 10 Mb/s.

#### 4.2.7.7 Algorytm sygnalizacyjny autonegoacji

Sieć IsoEthernet jest, jak już wspomniano, siecią o topologii gwiazdowej, w której urządzenia użytkowników są podłączone do układów dostępu AU. Algorytm sygnalizacyjny autonegoacji (ASA) (stanowiący nowy protokół w standardzie IEEE 802) umożliwia urządzeniom dołączanym do układów dostępu zgłaszenie możliwych trybów pracy i tym samym dobrą optymalnych parametrów sieci. Dzięki algorytmowi ASA układ AU potrafi automatycznie rozpoznać i dostosować się do parametrów dołączającego się urządzenia. Można również rekonfigurować pracę sieci (np. przechodzenie z pracy synchronicznej do wielousługowej w chwili wykrycia kart zgodnych z 10Base-T, i powrót do pracy synchronicznej po usunięciu tych kart).

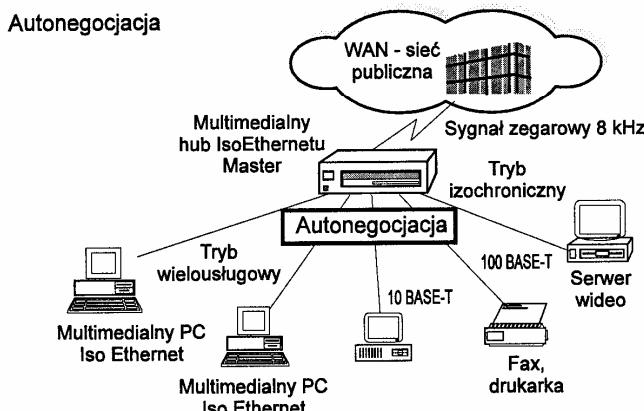
ASA umożliwia urządzeniom na obu końcach łącza zgłaszanie żądań i potwierdzeń użytkowania wspólnych trybów pracy i rezygnacji z tych trybów, które nie są dostępne. Jeśli dostępnych jest kilka trybów pracy, ASA pozwala na wybór tego trybu, którego priorytet jest wyższy (potrzebne informacje przechowywane są w odpowiedniej tablicy).

Rozwiązań IEEE 802.9 umożliwia łatwą współpracę z siecią rozległą WAN dzięki temu, że w trybach izochronicznym i wielousługowym sieć IsoEthernet

zapewnia dynamiczny przekaz ramek. Ta cecha pozwala na podporządkowanie pracy sieci lokalnej IsoEthernet zegarowi sieci WAN (8 kHz). Dzięki temu uzyskuje się przezroczysty styk między kanałami B sieci WAN, a siecią IsoEthernet.

W przypadku sieci IsoEthernet możliwe jest dołączenie do sieci wielu urządzeń, które mogą pracować w trybie master/slave. Aby uchronić się przed różnymi nieprawidłowościami w pracy sieci, np. wadliwą pracą aktualnego urządzenia typu master, każde inne urządzenie (uprawnione do pracy w trybie master/slave), pracujące dotychczas jako urządzenie typu slave, może automatycznie przejąć rolę nowego zarządcy sieci IsoEthernet. Wybór trybu pracy master/slave i wyznaczanie nowego urządzenia typu master realizowane jest przez jedną z procedur algorytmowi ASA.

Przykład sieci IsoEthernet wykorzystującej ASA w celu odpowiedniego skonfigurowania portów układu AU, w zależności od możliwości dołączonych urządzeń użytkowników, przedstawia rysunek 4.61. Porty układu AU zostały, dzięki ASA, skonfigurowane do pracy z urządzeniami różnych typów (synchroniczne i asynchroniczne), jak również do współpracy z siecią WAN (z zegarem odniesienia 8 kHz).



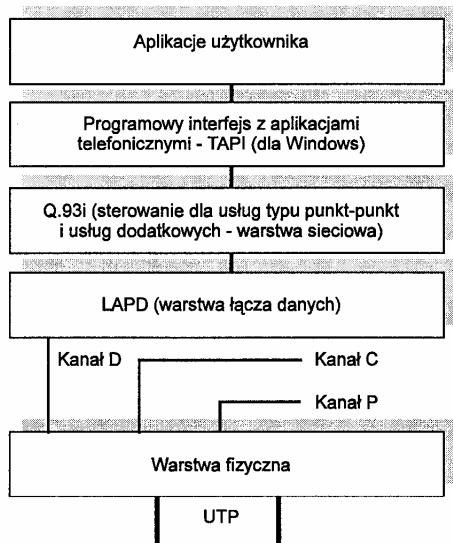
Rys. 4.61. Sieć IsoEthernet wykorzystująca algorytm sygnalizacyjny autonegoacji

#### 4.2.7.8 Procedury sygnalizacyjne w kanale C

Kanał C warstwy łączącej danych jest wykorzystywany do realizacji usług wymagających komutacji kanałów i, w zależności od konfiguracji, może pracować w dwóch trybach: wielousługowym i izochronicznym.

Mechanizmy sygnalizacyjne sieci IsoEthernet są podobne do mechanizmów sieci ISDN. Podobnie jak w ISDN, kanał C może składać się z pewnej liczby kanałów o przepustowości 64 kB/s (odpowiedniki kanałów B w ISDN). Zapewnienie odpowiedniej liczby kanałów odbywa się z wykorzystaniem procedur sygnaliza-

cyjnych. Procedury te są realizowane za pośrednictwem kanału D. Zostały one zdefiniowane w standardzie IEEE 802.9a w oparciu o rodzinę protokołów ITU Q.93x.



Rys. 4.62. Procedury sygnalizacyjne w IsoEthercie

Wśród procedur sygnalizacyjnych można wyróżnić (patrz rysunek 4.62):

- protokół dostępu do łącza w kanale D (ang. LAPD - *Link Access Protocol on the D-channel*),
- procedury współpracy użytkownika z siecią (ang. *IEEE 802.9a Q.93x User Network Interface UNI* (Q.93i)),
- procedury współpracy dla usług telefonicznych (ang. *Telephony Application Programmers Interface - TAPI for Windows*).

Procedury LAPD warstwy łącza są wykorzystywane do enkapsulacji wiadomości sygnalizacyjnych Q.93i i ich transportu kanałem D. Pozwalają one na:

- realizację jednego lub kilku połączeń w kanale D,
- szeregowanie ramek w warstwie łącza danych,
- kontrolę poprawności transmisji, formatu danych oraz wykrywanie błędów, w zależności od rodzaju połączenia,
- realizację i utrzymanie poprawności funkcjonowania protokołów warstwy łącza danych,
- zarządzanie warstwą łącza danych.

Procedury sygnalizacyjne Q.93i są wykorzystywane do sterowania połączeniami typu punkt-punkt, jak również do świadczenia usług dodatkowych. Zapewniają one zestawianie i nadzór usług realizowanych w kanale C. Wiadomości sygnalizacyjne są przesyłane między urządzeniami końcowymi oraz hubami IsoEthernetu. Usługi dodatkowe oferowane użytkownikom IsoEthernetu obejmują:

- transfer wywołań - informacje o wywołaniu (inicjowanym w kanale C) przesyłane są do innych urządzeń końcowych ISDN lub IsoEthernetu,
- podtrzymywanie wywołań - informacje o wywołaniu (inicjowanym w kanale C) mogą być opóźniane i ponawiane później,
- realizację konferencji - wielu użytkowników przyłączonych do sieci ISDN lub IsoEthernetu może uruchamiać sesje konferencyjne, korzystając z bloku sterowania połączeniami wielopunktowymi (ang. MCU - *Multipoint Control Unit*),
- realizację połączeń punkt-wielopunkt i wielopunkt-wielopunkt - dla sieci LAN/MAN istotnym aspektem będzie możliwość połączeń punkt-wielopunkt (poczta video- i audiofoniczna, jedno źródło informacji i wiele ujścia). Połączenia typu wielopunkt-wielopunkt umożliwiają obsługę wiadokonferencji.

Programowy interfejs aplikacji telefonicznych (TAPI) dla MS-Windows jest zaprojektowany podobnie do interfejsu użytkownika w ISDN (możliwa jest zatem współpraca urządzeń abonenckich ISDN i IsoEthernetu). TAPI zaprojektowano tak, aby przesłonić technologię przesyłu informacji. Aplikacje użytkownika korzystają z interfejsu TAPI. Ten z kolei wpływa na wywołania realizowane w sieci tak, aby osiągnąć zadowalającą jakość usług.

#### 4.2.7.9 IsoEthernet a ATM

ATM jest technologią opartą na przesyłaniu komórek o stałym, 53-oktetowym rozmiarze przez zestawione połączenia wirtualne; jest też technologią skalową, o przepustowości do 622 Mb/s, zapewniającą głównie obsługę ruchu połączego oraz współpracę z różnymi aplikacjami (CBR, VBR i ABR).

Pomiędzy ATM, a IsoEthernetem występują istotne podobieństwa. Technologie te używają podobnych protokołów sygnalizacyjnych opartych na Q.93x, jak również podobnych mechanizmów rozgłoszeniowych. Ułatwia to ewentualną współpracę sieci ATM z IsoEthernetem. W sieci ATM dla aplikacji transmisji mowy (połączenia rozmówne) wymagany jest specyficzny interfejs izochroniczny, zorientowany na obsługę ruchu zarówno CBR jak i VBR.

Komórki ATM mogą być w IsoEthercie w prosty sposób przenoszone kanałem C, dynamicznie konfigurowanym, zgodnie z wymaganiami ruchu ATM. Dzięki możliwościom multipleksacji izochronicznej i komutacji, AU może skonfigurować swoje kanały C tak, aby stały się łącznikiem dla komórek przesyłanych między siecią ATM, a IsoEthernetem (czyli siecią LAN).

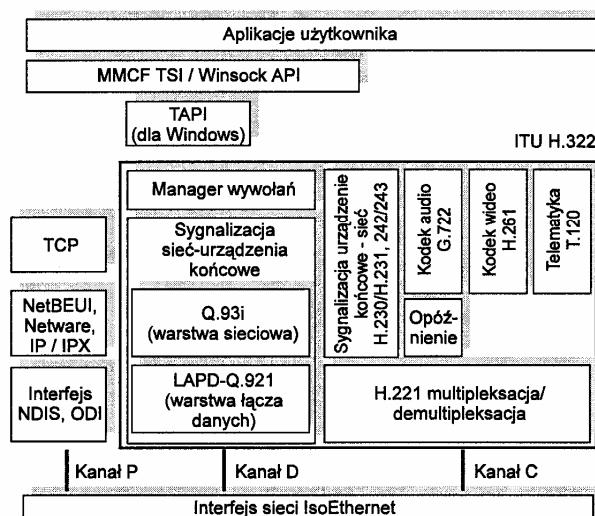
#### 4.2.7.10 Aplikacje multimedialne w IsoEthernecie

Idea komunikacji multimedialnej MMDC (ang. *Multimedia Desktop Collaboration*) oparta jest na połączeniu konferencji wideofonicznych z jednoczesnym przetwarzaniem informacji między wieloma użytkownikami.

Aplikacje MMDC są tworzone wg dwóch standardów zdefiniowanych przez grupę roboczą 15 ITU-T:

- standardu H.320 (1990), przeznaczonego dla usług sieci wąskopasmowej ISDN, oraz
- standardu H.322 (1995), będącego modyfikacją H.320 dla sieci lokalnych, które zapewniają identyczną jakość usług, co sieć ISDN.

Architektura aplikacji H.322 dla IsoEthernetu ma postać podaną na rysunku 4.63.



Rys. 4.63. Architektura aplikacji multimedialnych w sieci IsoEthernet

Obsługa transmisji pakietów wewnętrz kanału transmisyjnego (pracującego w oparciu o H.322) realizowana jest zgodnie z protokołem T.120. Protokół ten zapewnia przekaz plików, przesyłanie komunikatów i informacji sterujących konferencją. Warstwa TAPI umożliwia zestawianie i rozłączanie połączeń oraz realizację usług dodatkowych. TAPI komunikuje się z procedurami Q.931/Q.921 poprzez zarządcę wywołań (ang. *Call Manager*). Protokoły pakietowe TCP (dla sieci opartych na IP/IPX) są realizowane tak, jak w sieci Ethernet. Interfejsy dla usług transportowych zapewniane są przez warstwę leżącą między aplikacjami użytkownika i protokołami niższych warstw.

#### 4.2.7.11 Kierunki rozwoju IsoEthernetu

Kierunki rozwoju różnych technologii są w znacznym stopniu uwarunkowane postępami prac nad standaryzacją tych rozwiązań. Rozwój IsoEthernetu zmierza w stronę:

- współpracy pomiędzy układami dostępu AU (IEEE 802.9b),
- wprowadzenia do IsoEthernetu trybu przekazu asynchronicznego realizowanego w sieci ATM (IEEE 802.9e),
- zdalnego zasilania urządzeń abonenckich (IEEE 802.9f).

Technologia IsoEthernetu umożliwia dostęp użytkowników do usług multimedialnych oraz zapewnia współpracę z:

- Ethernetem (CSMA/CD 10Base-T), obecnie najbardziej popularnym rozwiązaniem dla sieci LAN,
- ATM i ISDN - rozwijającymi się nowoczesnymi technologiami,
- sieciami MAN (bez względu na tryb pracy).

#### 4.2.8 FDDI - Protokół dostępu do medium światłowodowego w sieci MAN

Protokół dostępu do medium światłowodowego FDDI (ang. *Fiber Distributed Data Interface*) stanowi standard amerykański opracowany przez ANSI (ANSI X3T9.5) i zaakceptowany przez ISO (ISO 9314). *Standard ten specyfikuje zasady dostępu do światłowodowej sieci pętlowej, będącej zwykle siecią podstawową, czy też tzw. siecią szkieletową (ang. backbone) dla połączeń pojedynczych stacji lub odległych sieci LAN.*

##### 4.2.8.1 Podstawowe parametry

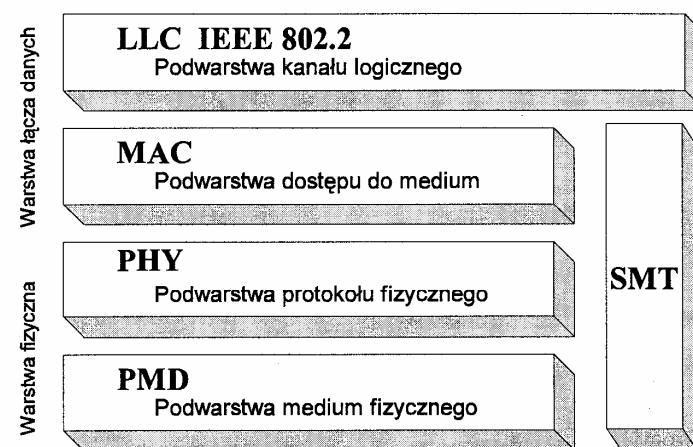
Standard FDDI specyfikuje zasady pracy sieci z podwójną pętlą światłowodową pozwalającą na prowadzenie transmisji informacji z szybkością 100 Mb/s w każdej pętli. Zastosowanie światłowodów jednomodowych umożliwia tworzenie sieci o długościach magistrali do 200km, bądź nawet większych, z maksymalną liczbą stacji rzędu 1000. Tym samym standard FDDI jest typową propozycją dla sieci miejskich (metropolitalnych), czyli sieci typu MAN.

Specyfikacja FDDI ANSI X3T9.5 obejmuje cztery zasadnicze części. Są to:

- Podwarstwa **PMD** (ang. *Physical Medium Dependent Layer*) kanału fizycznego - definiująca długości fali światła i parametry toru światłowodowego.
- Podwarstwa **PHY** (ang. *Physical Layer Protocol*) protokołu warstwy fizycznej - definiująca sposoby kodowania i dekodowania sygnałów, synchronizację pracy sieci, zasady tworzenia ramek itp. Dla protokołu tej warstwy istnieją rozwiązania w postaci gotowych układów scalonych.

- Podwarstwa **MAC** (ang. *Medium Access Control*) - specyfikująca zasady dostępu do medium, formaty przesyłanych ramek, zasady obsługi tokena, sposoby adresacji, metody zapewnienia podwyższonej niezawodności pracy stacji i sieci.
- Blok **SMT** (ang. *Station Management*) protokołów zarządzania pracą stacji - zapewniający kontrolę działania sieci jako pewnej całości, procedury inicjowania pierścienia oraz nawiązywania połączeń w przypadku wystąpienia awarii.

Relacje pomiędzy poszczególnymi elementami funkcjonalnymi modelu ANSI ilustruje rysunek 4.64.



Rys. 4.64. Specyfikacja ANSI a model odniesienia ISO-OSI

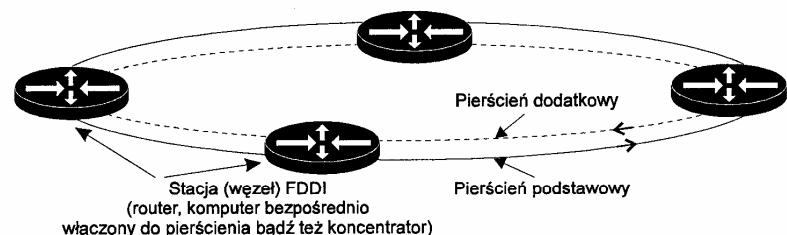
FDDI wykorzystuje oprogramowanie IEEE 802.2 do realizacji sterowania przepływem ramek w podwarstwie LLC oraz standardy ISO dla warstw wyższych. *Stosowany w FDDI protokół podwarstwy MAC oparty jest na standardzie IEEE 802.5 (i częściowo IEEE 802.4) z pewnymi modyfikacjami, związanymi z większymi szybkościami pracy.* Dotyczą one między innymi zastosowania zmodyfikowanej metody czasowego tokenowego sterowania dostępem oraz nieco innych niż w IEEE 802.5 zasad przechwytywania i uwalniania tokena.

*W nowszej wersji standardu FDDI, określonej mianem FDDI II, proponowany jest hybrydowy system transmisji pozwalający na realizację pierścienia szcześniowego z ramkowaniem (ang. slotted ring). System FDDI II zapewnia obsługę ruchu izochronicznego oraz ruchu synchronicznego i asynchronicznego, czyli przesyłanie obrazów wideo, sygnałów mowy i danych w jednej sieci, poprzez wydzielanie podkanalów cyfrowych dla połączeń wideofonicznych. FDDI II pozwala na utworzenie do 16-tu dynamicznie przydzielanych kanałów szerokopas-*

mowych o przepustowościach 6.144Mb/s oraz jednego kanału o przepustowości 0.708 Mb/s, zarezerwowanego do celów sterowania oraz obsługi ruchu synchronicznego i asynchronicznego.

#### 4.2.8.2 Topologia sieci i typy stacji

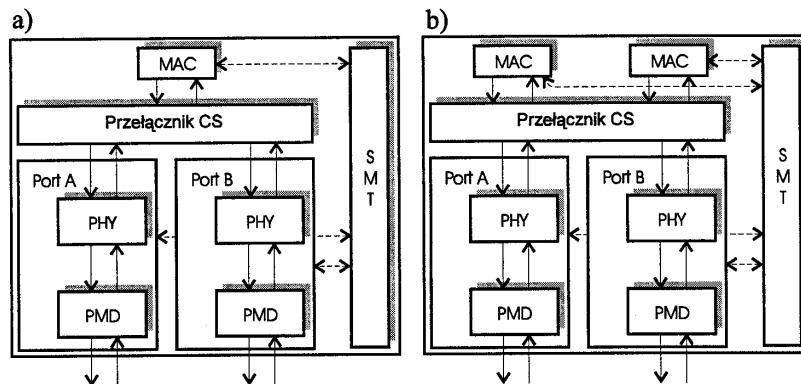
Każdy standard definiuje swoją własną topologię. W przypadku sieci Ethernet i Token Bus jest to magistrala, w sieci ARCnet połączenia stacji tworzą gwiazdę. Z kolei w standardzie Token Ring stacje są rozlokowane na obwodzie pierścienia. W przypadku standardu FDDI wyróżnić można dwa pierścienie: podstawowy (ang. *primary ring*) i dodatkowy (ang. *secondary ring*). Pierścień podstawowy służy do transmisji danych, zaś pierścień dodatkowy stanowi połączenie rezerwowe. Należy podkreślić fakt, że standard nie przewiduje wykorzystania drugiego pierścienia w celu zwiększenia przepustowości sieci podczas normalnej jej pracy. Przykładowy pierścień FDDI pokazano na rysunku 4.65.



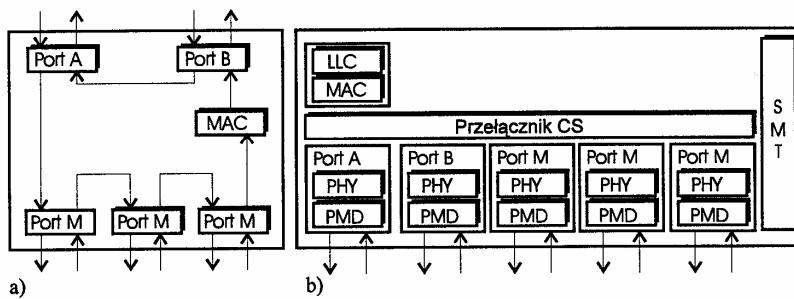
Rys. 4.65. Przykładowy pierścień FDDI

Podwójny pierścień może zawierać kilka typów urządzeń, zwanych stacjami lub koncentratorami. W standardzie FDDI - ze względów oszczędnościowych - nie każda stacja musi być połączona do obydwu pierścieni. Definiuje się przy tym następujące typy stacji i koncentratorów:

- **DAS** (ang. *Dual-Attachment Station*) - stacja przyłączona bezpośrednio do obydwu pierścieni (tzw. stacja typu A). Stacja DAS posiada 2 porty tj: dwie pary obiektów warstw PMD i PHY, obiekt (obiekty) MAC, przełącznik CS (ang. *Configuration Switch*) i jeden obiekt SMT (oprogramowanie lub układ scalony). W stacji posiadającej dwa obiekty MAC obsługujące dwa pierścienie, możliwa jest ciągła transmisja w obu pierścieniach i zwiększenie przepustowości do 200 Mb/s. Schemat blokowy stacji DAS przedstawiono na rysunku 4.66.
- **DAC** (ang. *Dual-Attachment Concentrator*) - koncentrator umożliwiający przyłączenie innych stacji do podwójnego pierścienia FDDI. W większości koncentratorów DAC zaimplementowany jest protokół zarządzania SNMP (ang. *Simple Network Management Protocol*). Schemat blokowy koncentratora (stacji) DAC przedstawiono na rysunkach 4.67a i b.

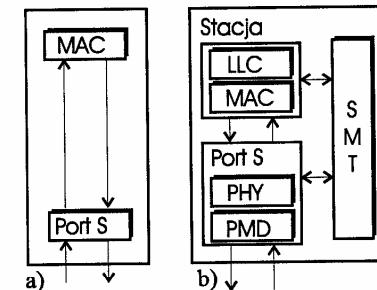


Rys. 4.66. Schemat blokowy stacji DAS: a) z jednym obiektem MAC, b) z dwoma obiektami MAC



Rys. 4.67. Schemat blokowy koncentratora DAC: a) przykładowy schemat połączeń portów stacji DAC, b) przykładowa architektura wewnętrzna stacji DAC (liczba obiektów LLC/MAC w stacji DAC może się zmieniać od 0 do 2)

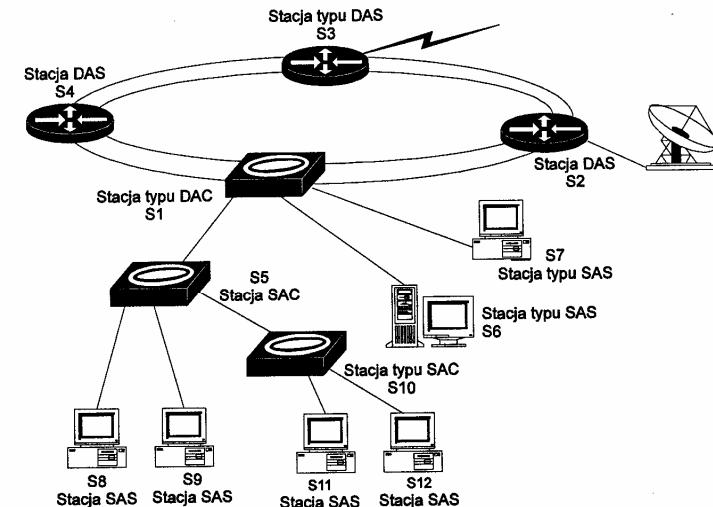
- SAS (ang. *Single-Attachment Station*) - stacja tego typu nie może być włączona bezpośrednio do pierścienia głównego. Dołączenie stacji SAS do sieci dokonuje się jedynie za pośrednictwem koncentratora (stacja SAS jest tzw. stacją typu B). Stacja SAS używana jest w celu obniżenia kosztów instalacji sieci, a także, gdy należy zapewnić łatwość włączania lub usuwania stacji z pętli. Schemat blokowy stacji SAS przedstawiono na rysunku 4.68. Stacja SAS ma jedynie parę obiektów warstw PMD i PHY oraz jeden obiekt MAC (i jeden obiekt LLC).
- SAC (ang. *Single-Attachment Concentrator*) - koncentrator umożliwiający tworzenie topologii drzewiastej. Posiada jeden port S i kilka M. Podłączony jest tylko do jednego pierścienia za pośrednictwem koncentratora DAC. Może, ale nie musi posiadać obiektów MAC, a także implementację SNMP.



Rys. 4.68. Schemat blokowy stacji SAS: a) schemat połączeń wewnętrznych, b) przykładowa architektura wewnętrzna stacji SAS

Stacje (węzły) połączone są z pierścieniem oraz, między sobą, poprzez odpowiednie porty:

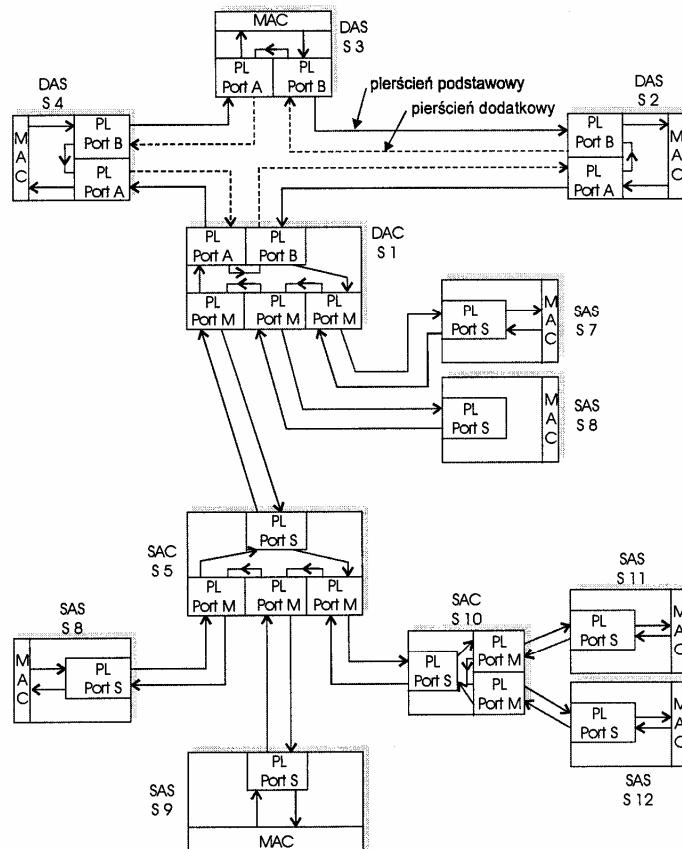
- port A - definiowany jest jako ten, do którego dochodzi sygnał z pierścienia podstawowego, a wychodzi do pierścienia dodatkowego,
- port B - definiowany jest jako ten, do którego dopływa sygnał z pierścienia dodatkowego, a wypływa do pierścienia podstawowego,
- port M - jest portem występującym w koncentratorach, a którego zadanie polega na dystrybucji pakietów do innych stacji,
- port S - jest portem odbierającym ramki z portu M, występuje on w stacjach SAS dołączonych do koncentratorów.



Rys. 4.69a. Przykładowa ilustracja pierścienia FDDI z systemami wewnętrznymi wykorzystującymi różne typy stacji z zaznaczeniem typów stacji

Wykorzystując opisane powyżej typy stacji (węzłów sieci) można zaprojektować szereg różnych wielopoziomowych rozwiązań sieci. Są to przykładowo:

- sieć z pojedynczym koncentratorem z dołączonymi stacjami,
- sieć z drzewem koncentratorów - rozwiązanie użyteczne do przyłączenia większej liczby urządzeń często wykorzystywanych przez użytkowników. Konfiguracja ta zapewnia łatwość dodawania lub usuwania stacji, a także możliwości zmiany ich lokalizacji,
- podwójny pierścień - stosowany jako szkielet sieci MAN, w której każda stacja FDDI traktowana jest jako most bądź router,
- podwójny pierścień z drzewami koncentratorów.



Rys. 4.69b. Przykładowa ilustracja pierścienia FDDI z systemami wewnętrznymi wykorzystującymi różne typy stacji z podaniem schematu połączeń stacji (warstwa fizyczna PL/WF uwzględnia obiekty PHY i PMD)

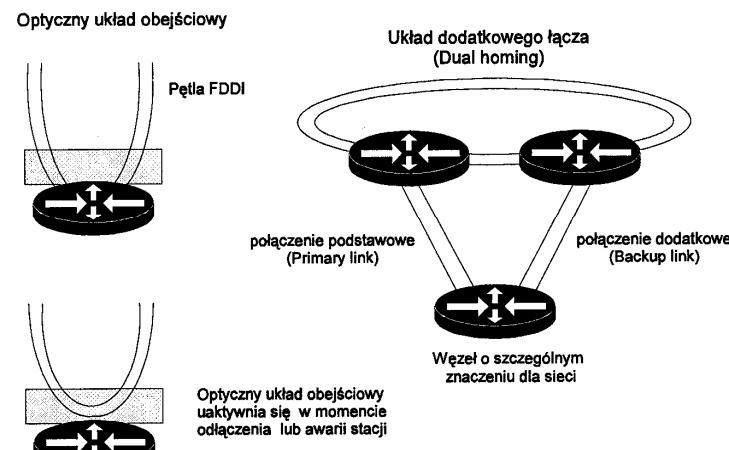
Przykładową strukturę pierścienia z systemami wewnętrznymi z wykorzystaniem poszczególnych typów stacji pokazano na rysunku 4.69.

#### 4.2.8.3 Niezawodność pracy sieci

W przypadku awarii stacji lub uszkodzenia światłowodu pierścień jest automatycznie rekonfigurowany. Nadzór nad rekonfiguracją sieci sprawuje system zarządzania, będący częścią SMT. Poza tym FDDI ma też i inne standardowe mechanizmy przywracania prawidłowej pracy sieci.

Podstawowym układem wykorzystywanym przy rekonfiguracji sieci jest optyczny układ obejściowy (ang. optical bypass). Urządzenie to w momencie uszkodzenia stacji lub braku zasilania "zamyka" połączenie światłowodowe, w taki sposób, że sygnał ze stacji poprzedniej przechodzi bezpośrednio do stacji następnej. Układ może być uaktywniony zarówno przez stację uszkodzoną lub też stację sąsiednią, jak też przez operatora sieci. W wypadku stosowania tego typu urządzeń należy pamiętać o tym, że nowe połączenie między czynnymi stacjami pętli musi spełniać warunki "odległościowe i tłumieniowe". Urządzenie obejściowe wprowadza 2.5 dB straty mocy.

Innym elementem zapewniającym łatwość rekonfiguracji strukturalnej jest układ dodatkowego łącza (ang. Dual Homing). Jest to sposób na zabezpieczenie dostępu do pierścienia dla urządzenia mającego duże znaczenie dla użytkowników (komputer typu mainframe, router). W tym celu wprowadzane jest dodatkowe połączenie (ang. backup link). Staje się ono aktywne w momencie wystąpienia awarii połączenia podstawowego (ang. primary link). Optyczny układ obejściowy oraz układ dodatkowego łącza przedstawiono na rysunku 4.70.



Rys. 4.70. Stosowane zabezpieczenia

#### 4.2.8.4 Warstwa fizyczna w FDDI

Warstwa fizyczna definiuje charakterystyki optyczne i mechaniczne światłowodu, poziomy mocy optycznej, dynamiczny zasięg odbiorników optycznych oraz metodę kodowania 4B/5B.

Do nadawania i odbioru sygnałów stosowane są zwykle dwa światłowody umieszczone w jednej osłonie; długość fali przesyłanych sygnałów wynosi przy tym 1300 nm.

Stosowane w FDDI kodowanie 4B/5B zapewnia wysoką efektywność transmisji (80% w porównaniu z 50% dla kodu Manchester). Metoda 4B/5B oznacza, że ciągi czterobitowe są kodowane symbolami 5-cio bitowymi - zgodnie z przyporządkowaniem pokazanym w tabeli 4.9.

Tabela 4.9. Kod 4B/5B i symbole zdefiniowane przez standard FDDI

Zakodowana informacja	Symbol	Znaczenie
<b>Dane</b>		
11110	0	0000
01001	1	0001
10100	2	0010
10101	3	0011
01010	4	0100
01011	5	0101
01110	6	0110
01111	7	0111
10010	8	1000
10011	9	1001
10110	A	1010
10111	B	1011
11010	C	1100
11011	D	1101
11100	E	1110
11101	F	1111
<b>Symboli stanu linii</b>		
00000	Q	Quiet
11111	I	Idle
00100	H	Halt
<b>Oznaczenie początku ramki</b>		
11000	J	Pierwsza część SD
10001	K	Druga część SD
<b>Oznaczenia końca ramki</b>		
01101	T	

Tabela 4.9. Kod 4B/5B i symbole zdefiniowane przez standard FDDI (c.d.)

Zakodowana informacja	Symbol	Znaczenie
<b>Wskaźniki</b>		
00111	R	ustawia logiczne zero
11001	S	ustawia logiczną jedynkę
<b>Błędy</b>		
00001	V lub H	
00010	V lub H	
00011	V	
00101	V	
00110	V	
01000	V lub H	
01100	V	
10000	V lub H	

#### 4.2.8.5 Podwarstwa MAC

Podobnie jak w przypadku omawianych wcześniej standardów IEEE serii 802 dla sieci LAN, w tym 802.3, 802.4, 802.5, podwarstwa MAC zdefiniowana w standardzie FDDI realizuje szereg ważnych funkcji. Najistotniejszą z nich jest zapewnienie zdecentralizowanego dostępu do medium fizycznego. Inne funkcje to tworzenie ramek, a także kontrola poprawności transmisji ramki.

Usługi podwarstwy dostępu w podstawowym trybie jej pracy, tj. trybie bezpołączniowym, są udostępniane za pośrednictwem trzech operacji elementarnych :

- 1. żądania - MA\_UNITDATA.request
- 2. zawiadomienia - MA\_UNITDATA.indication
- 3. potwierdzenia - MA\_UNITDATA.confirmation (opcjonalnie)

Żądanie może być wygenerowane przez obiekt warstwy wyższej - LLC. Parametry operacji żądania transmisji, oprócz elementów takich jak adres docelowy, dane i wartości pola FC, uwzględniają też wymaganą klasę usług. FDDI definiuje dwie klasy usług: przesyłanie synchroniczne i asynchroniczne.

Zawiadomienie jest wynikiem odebrania przez obiekt podwarstwy dostępu ramki zaadresowanej do obsługiwanej przez ten obiekt punktu udostępniania usług. Parametry zawiadomienia to adres źródłowy, docelowy, dane i status odbioru.

#### Usługi podwarstwy MAC dla podwarstwy LLC

Poniżej wyspecyfikowane są prymitywy operacyjne (operacje elementarne) pozwalające podwarstwie LLC na swobodną wymianę jednostek danych LLC-SDU pomiędzy obiektami LLC w różnych stacjach.

- MA\_UNITDATA.request

Operacja elementarna żądania transmisji, realizowana przez obiekt warstwy LLC w momencie zgromadzenia danych wygenerowanych przez warstwę wyższą lub przez samą podwarstwę LLC.

Odbiór prymitywu MA\_UNITDATA.request przez podwarstwę MAC powinien spowodować dodanie do wiadomości LLC-CDU wszystkich elementów charakterystycznych dla podwarstwy MAC (DA, SA, elementy kontrolne) i wysłanie tak uformowanej ramki do warstwy fizycznej.

- **MA\_UNITDATA.indication**

Prymityw kierowany do obiektu podwarstwy LLC w momencie odbioru przez obiekt MAC ramki LLC adresowanej do danej stacji.

- **MA\_UNITDATA\_STATUS.indication**

- **MA\_TOKEN.request**

Prymityw ten generowany jest przez obiekt LLC w przypadku konieczności zrealizowania szybkiej transmisji jednostki dianych LLC-SDU. Odbiór tego prymitywu przez obiekt MAC powinien spowodować przechwytcenie tokenu (może to być token normalny lub zastrzeżony z podaniem poziomu priorytetu). Po jego przechwytceniu MAC przechodzi do stanu „biernej” transmisji (stan określany jako T2) nadając symbole Idle, aż do momentu otrzymania MA\_UNITDATA.request. Jeżeli jednak wcześniej upłynie tzw. czas TRT obiegu tokenu, to MAC ponownie „wprowadza do pętli token o przechwyconym priorytecie”.

#### Usługi podwarstwy PHY dla podwarstwy MAC

Usługi przekazu bitowego warstwy fizycznej oferowane są za pośrednictwem styku warstw MAC i PHY. Styk ten pozwala podwarstwie MAC na wymianę ramek (MAC-PDU) pomiędzy odpowiednimi obiektami podwarstwy MAC w dwóch lub więcej stacjach.

- **PH\_UNITDATA.request**

Operacja definiuje przekaz danych od MAC do PHY.

- **PH\_UNITDATA.indication**

Operacja definiuje przekaz danych od PHY do MAC. Obiekt podwarstwy PHY wysyła PH\_UNITDATA.indication, gdy tylko zdekoduje kolejny symbol. Podwarstwa MAC w momencie otrzymania danych powinna je przetworzyć i wygenerować PH\_UNITDATA.request.

- **PH\_UNITDATA\_STATUS.indication**

Podwarstwa PHY wysyła PH\_UNITDATA\_STATUS.indication do podwarstwy MAC w odpowiedzi na każdą PH\_UNITDATA.request. Celem takiej operacji jest synchronizacja przesyłu danych, wychodzących z podwarstwy MAC do warstw wyższych, z danymi przychodząymi. Odbiór tego prymitywu umożliwia podwarstwie MAC realizowanie następnej operacji PH\_UNITDATA.request.

- **PH\_INVALID.indication**

PHY generuje operację w momencie wykrycia błędów. Podwarstwa MAC powinna zasygnalizować błąd i odpowiednio zmienić swój stan.

#### Usługi podwarstwy MAC dla procesów SMT

Poniżej opisane są prymitywy (operacje podstawowe) przesyłane na styku odpowiednich obiektów SMT i MAC. Prymitywy te używane są przez lokalny obiekt SMT w celu monitorowania i kontrolowania operacji podwarstwy MAC.

- **SM\_MA\_INITIALIZE\_PROTOCOL.request**

Operacja generowana w momencie rekonfiguracji pierścienia. Parametry tej operacji zawierają wszystkie potrzebne zmienne, liczniki i flagi. Podwarstwa MAC otrzymując tę operację powinna definitywnie ustalić wszystkie parametry i przesłać stosowne potwierdzenie SM\_MA\_INITIALIZE\_PROTOCOL.confirm.

- **SM\_MA\_CONTROL.request**

Prymityw używany przez lokalny obiekt SMT do kontroli działań podwarstwy MAC.

- **SM\_MA\_STATUS.indication**

Operacja realizowana przez MAC w celu poinformowania SMT o błędach.

- **SM\_MA\_UNITDATA.request**

Operacja elementarna definiująca przekaz jednej lub więcej jednostek danych SDU (ang. *Service Data Unit*) pochodzących od SMT, generowana po przygotowaniu danych do przesłania do innego obiektu SMT. Podwarstwa MAC powinna dodać do jednostki SDU wszystkie swoje elementy (SA, DA, elementy kontrolne) i przekazać tak uformowaną ramkę do warstw niższych.

- **SM\_MA\_UNITDATA.indication**

Operacja zawiadamiająca obiekt SMT o przybyciu ramki adresowej do SMT. Jednym z elementów prymitywu jest parametr reception\_status informujący o poprawności ramki (FCS, długość, FS)

- **SM\_MA\_UNITDATA\_STATUS.indication**

Operacja generowana przez podwarstwę MAC w odpowiedzi na SM\_MA\_UNITDATA.request.

- **SM\_MA\_TOKEN.request**

Operacja generowana przez SMT w celu przechwytcenia tokenu.

#### 4.2.8.6 Format tokena i ramki

Każdy standard sieciowy definiuje formaty stosowanych ramek. W FDDI definiowane są takie jednostki informacyjne jak token, ramki informacyjne oraz ramki

sterująco-utrzymaniowe. Podstawowe znaczenie odgrywa przy tym ramka informacyjna. W FDDI ramka ta składa się z 9 pól. Może ona przenosić dane użytkownika, a także informacje podwarstw MAC, LLC i SMT. Strukturę ramki informacyjnej i tokena ilustruje rysunek 4.71.

Token:

Preambuła	SD	TFC	ED
-----------	----	-----	----

Ramka:

Preambuła	SD	FC	DA	SA	DANE	FCS	ED	FS
-----------	----	----	----	----	------	-----	----	----

Rys. 4.71. Format TOKENa i ramki FDDI

**Sterowanie dostępem do medium realizowane jest za pomocą tokena.** Token jest specjalnym typem ramki krążącej wokół pętli. Pole kontrolne TFC pozwala na szybkie odróżnienie tokena od ramki informacyjnej. Ciąg symboli charakteryzujący token do JK80TT (patrz tabela 4.9). **Przejęcie tokena uprawnia stację do przesłania ramki (ramek) informacyjnej.** Standard ANSI FDDI definiuje dwa rodzaje tokenów: zwykły (niezastrzeżony) i zarezerwowany (zastrzeżony) (ang. *restricted*). Pierwszy z nich wykorzystywany jest podczas normalnej pracy, gwarantująccej sprawiedliwy dostęp do łącza i bezkolizyjne przesyłanie ramek. Token zastreżony używany jest do przydziału całości pasma dla dwóch stacji dokonujących wymiany bardzo dużych porcji informacji. Czas, przez który stacja może nadawać w tym trybie, jest ustalany i kontrolowany przez podwarstwę SMT.

Zarówno token jak i ramka rozpoczynają się polem preambuły, o minimalnej długości 16 bajtów, zawierającej symbole *Idle*. Warstwy fizyczne PHY poszczególnych stacji mogą zmieniać długość preambuły, gdyż ma ona za zadanie synchronizację zegarów lokalnych. Jeśli preambuła zawiera mniej niż 12 symboli, ramka nie może zostać zaakceptowana przez żadną stację.

Kolejne pola tokena/ramki mają następujące znaczenie:

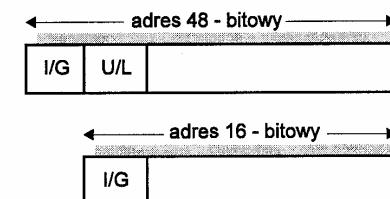
- SD (ang. *Starting Delimiter*) - pole to stanowi ciąg początku ramki. Jest ono kodowane jako dwa czterobitowe symbole J i K. Każda poprawna ramka powinna rozpoczynać się taką sekwencją.
- TFC (ang. *Token Frame Control*) - pole to, podobnie jak i FC (ang. *Frame Control*) ma postać bajtu CLFFZZZZ, gdzie C mówi nam, czy jest to transmisja synchroniczna (1) czy asynchroniczna (0), L wskazuje na adres 16 bitowy (0) lub 48 bitowy (1), a po kombinacji bitów poznajemy, czy jest to ramka LLC, MAC, SMT, czy też token zarezerwowany:

0X000000

ramka pusta (jej zawartość powinna być przez stacje zignorowana)

10000000	token niezastrzeżony
11000000	token zarezerwowany (zastrzeżony)
0L000001 do 0L001111	ramki SMT
1L000001 do 1L011111	ramki MAC
1L000010	ramka MAC sygnalizacyjna ( <i>beacon</i> )
1L000011	ramka MAC żądania ( <i>claim</i> )
CL01r000 do CL01r111	ramka LLC
r=0, X=0 lub X=1	

- DA (ang. *Destination Address*) - pole to specyfikuje, do kogo jest adresowana ramka. Przeznaczeniem może być pojedyncza stacja lub grupa stacji. W sieci mogą być stosowane adresy 16 lub 48 bitowe, zgodnie z przyjętą przez IEEE metodą adresacji (patrz rysunek 4.72).



I/G bit adresowania indywidualnego (0) lub grupowego (1)  
U/L bit adresowania globalnego (0) lub lokalnego (1)

Rys. 4.72. Format adresów

- SA (ang. *Source Address*) - pole to specyfikuje nadawcę ramki. Zasady adresacji są takie same jak w przypadku adresata.
- INFO - w tym polu przechowywane są właściwe informacje, które mają trafić do odbiorcy. W polu tym przesyłane są także dane wymieniane pomiędzy podwarstwami MAC, LLC i SMT. Maksymalna długość pola danych to 4500 bajtów (9000 znaków 4-ro bitowych).
- FCS (ang. *Frame Check Sequence*) oznaczane też jako pole CRC (ang. *Cyclic Redundancy Check*) - pole to odpowiedzialne jest za wykrywanie błędów. Procedura wykrywania błędów realizowana jest z wykorzystaniem kodu cyklicznego opartego na wielomianie  
 $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ .
- Zabezpieczenie kodowe obejmuje pola FC, DA, SA, INFO i samo pole FCS.
- ED (ang. *Ending Delimiter*) - w polu tym umieszczane są symbole T charakteryzujące koniec ramki (dwa symbole T dla tokenu, jeden dla ramki). Całkowita długość ramki informacyjnej może wynosić około 4500 bajtów. W FDDI istnieje przy tym możliwość transmisji więcej niż 1 ramki po przechwytceniu tokenu.

- FS (ang. *Frame Status*) - pole to określa status ramki, który pozwala na szybką realizację powiadomienia ACK. Status charakteryzowany jest przez trzy symbole: E - wskaźnik detekcji błędu, A - wskaźnik rozpoznania adresu zmieniany na S przez stację, która rozpozna adres odbiorcy jako swój własny, C - wskaźnik skopiowania ramki, ustawiany przez stację kopiącą ramkę do swojego bufora. Każdy wskaźnik może być reprezentowany przez dwa symbole R (ang. *Reset*) lub S (ang. *Set*).

E - wykrycie błędu. Wskaźnik E ustawiany jest na R przez stację nadającą. Każda inna stacja może ustawić wskaźnik na S, w momencie wykrycia błędu.

A - wskaźnik rozpoznania adresu. Jeśli jakakolwiek stacja rozpozna swój adres (na polu DA), ustawia wskaźnik na S.

C - wskaźnik skopiowania ramki. Jeśli jakakolwiek stacja rozpoznała swój adres i skopiowała ramkę do swojego bufora odbiorczego, ustawia wskaźnik na S.

Wskaźniki pozwalają nadawcy, w momencie "pochłonięcia ramki", po jej „powrocie” z pętli, na rozróżnienie trzech stanów:

1. Stacja docelowa (adresat ramki) nieobecna lub nieaktywna;
2. Stacja aktywna, ale ramka nie została skopiowana (błędny);
3. Ramka osiągnęła cel i została skopiowana do bufora adresata.

#### 4.2.8.7 Ważniejsze zmienne, liczniki i flagi stosowane w procedurach FDDI

Realizacja procedur sterowania dostępem do medium wymaga, w przypadku FDDI, zdefiniowania i używania w każdej stacji pewnej liczby zmiennych i liczników. Pozwalają one określić np. czas przez jaki stacja może nadawać ramki. Przekroczenie wartości progowych liczników powoduje uruchomienie stosowanych alarmów. Pociąga to za sobą odpowiednie działania korekcyjne.

- Zmienna D\_Max - określa maksymalne opóźnienie w pierścieniu będące maksymalnym czasem obiegu SD (*Starting Delimiter*) wokół pętli. Czas ten składa się z opóźnienia propagacyjnego i opóźnienia w poszczególnych stacjach. Standardowo D\_Max = 1.617 ms.
- Zmienna T\_Req - oznacza czas obiegu tokena żądany przez daną stację. Podczas procesu żądania tokena stacja deklaruje, jako wartość tej zmiennej czas, jaki stacja chciałaby, aby upłynął do następnego przybycia tokena. Innymi słowy, jak szybko ma krążyć token w pierścieniu, aby zaspokoić potrzeby stacji. Stacja żądająca najszybszej rotacji tokena wygrywa proces żądania.
- Zmienna T\_Opr - wyznacza czas "operacyjny" (nominalny) obiegu tokena, na który zgadzają się wszystkie stacje. Stacja wygrywająca proces żądania tokena przepisuje wartość swojej zmiennej T\_Req do zmiennej

T\_Opr. Wartość ta staje się tzw. Nominalnym Czasem Obiegu Tokena TTRT (ang. *Target Token Rotation Time*). TTRT musi przy tym spełniać nierówność

$$\tau + F_{Max} + Token\_Time + \sum SA_i \leq TTRT$$

gdzie

$\tau$	- czas propagacji w pętli FDDI
$F_{Max}$	- maksymalny czas transmisji ramki tj. 9000 symboli + 16 symboli preambuły $F_{Max} = 0.361$ ms
$Token\_Time$	- czas potrzebny na transmisję tokenu i preambuły $Token\_Time = 0.00088$ ms
$SA_i$	- czas potrzebny na transmisje ramek synchronicznych. Może on być różny dla poszczególnych stacji. Jest on przydzielany z pomocą protokołu SMT, który sprawdza też, czy podana powyżej nierówność jest spełniona.

- Zmienna T\_Max - opisuje maksymalną wartość TTRT. Zmienna ta wprowadzona jest w celu narzucenia górnej granicy czasu obiegu pętli (i jednocześnie czasu, po którym dokonywana jest renegotiacja wartości TTRT). Standardowo T\_Max wynosi 165 ms.
- Zmienna T\_Min definiuje minimalną wartość TTRT. Wartość T\_Min gwarantuje efektywne wykorzystanie pierścienia i jego prawidłową pracę. Standardowo T\_Min wynosi 4 ms.
- Licznik TRT (ang. *Token Rotation Time*) - licznik ten służy do mierzenia czasu pomiędzy kolejnymi przybyciami tokenu do stacji. Do licznika tego w przypadku poprawnej pracy pierścienia, zapisywana jest wartość TTRT. W przeciwnym wypadku, tj. gdy pierścień nie funkcjonuje poprawnie, wprowadzana jest wartość T\_Max. Działanie tego licznika zostanie omówione szczegółowo przy okazji omawiania zasad dostępu do medium.
- Licznik THT (ang. *Token Holding Time*) - licznik THT pozwala na kontrolę czasu przez jaki stacja może transmitować ramki asynchronouszne. W momencie przybycia tokenu, do THT ładowana jest wartość pozostająca w liczniku TRT.
- Licznik TVX - licznik ten mierzy odstęp czasu pomiędzy dwiema kolejnymi ramkami. Definiuje się go w celu przyśpieszenia standardowego czasu negocjacji wartości TTRT i/lub rekonfiguracji sieci ( $2*TTRT = 330$  ms). Wartość TVX jest ustawiana na  $2*TTRT$  w momencie otrzymania ramki. Jeśli TVX upłynie, oznacza to, że żadna ramka, włączając w to token, nie nadeszła i należy rozpocząć proces rekonfiguracji.

$$TVX > \text{Max}(D_{\text{Max}}, F_{\text{Max}}) + \text{Token\_Time} + F_{\text{Max}} + S_{\text{Min}} > 2.35 \text{ ms}$$

$S_{\text{Min}}$  - minimalny czas pozwalający na odtworzenie błędnych informacji.

$$S_{\text{Min}} = F_{\text{Max}} + L_{\text{Max}} = 0.3645 \text{ ms.}$$

$L_{\text{Max}}$  - maksymalny czas po przechwyceniu tokena, po którym stacja musi rozpocząć nadawanie ramek.

- Zmienna Late\_Ct (ang. *Late Counter*) - zmienna ta wykorzystywana jest do kontroli czasu obiegu tokena. Jeśli licznik TRT zmaleje do zera przed przybyciem tokena, flaga (wartość Late\_CT) jest zwiększana o 1 (z 0 na 1 lub z 1 na 2). Znaczenie tej flagi opisane zostanie przy okazji omawiania zasad dostępu do medium.

#### 4.2.8.8 Protokół wymiany informacji w FDDI

*Protokół wymiany informacji stosowany w FDDI oparty jest na standardowych rozwiązańach IEEE 802.5 i 802.4.* Istnieją jednakże dwie podstawowe różnice, związane ze zwiększoną przepływnością sieci FDDI. Pierwsza z nich to rozpoczęcie nadawania ramek już w chwili rozpoznania tokena. Druga to "uwalnianie" tokena w chwili zakończenia transmisji ramki nawet wtedy, gdy stacja nie zaczęła jeszcze odbierać wysłanej przez siebie ramki.

#### Zasady przydziału dostępu do medium transmisyjnego

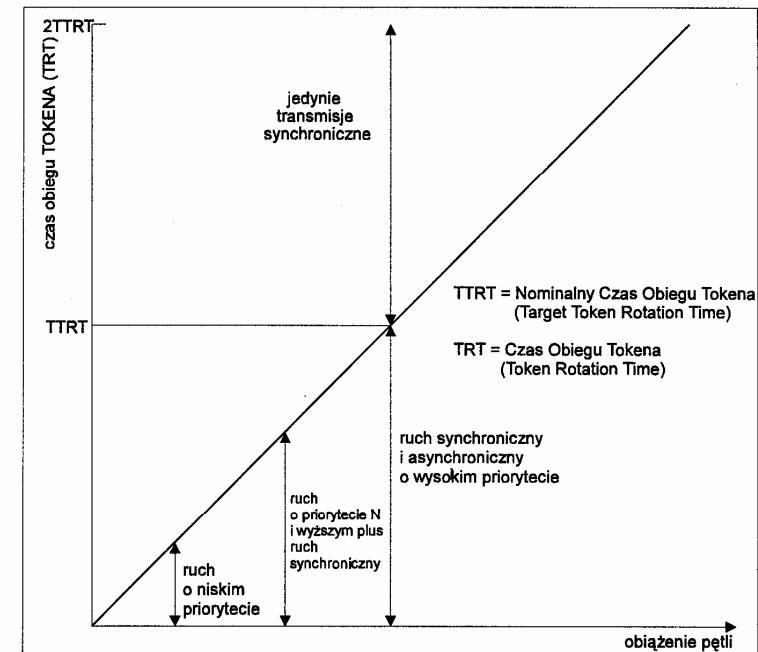
FDDI definiuje dwa rodzaje ruchu: ruch synchroniczny i asynchroniczny oraz dwie procedury obsługi tych typów ruchu.

*Procedura obsługi ruchu synchronicznego gwarantuje określona przepływność i ograniczone opóźnienie w dostępie.* Jest ona szczególnie użyteczna dla aplikacji wymagających dostępu do medium o określonej przepływności (głos, sygnały wideo, informacje służące do kontroli produkcji), tj. aplikacji realizowanych zwykle w czasie rzeczywistym.

Z kolei *procedura obsługi ruchu asynchronicznego umożliwia przydział stacjom sieci części przepływności nie wykorzystanej na obsługę ruchu synchronicznego.* Procedura ta jest aktywniana w momencie malego i średniego ruchu w sieci. Nie gwarantuje ona pełnej obsługi ruchu asynchronicznego w przypadku dużego obciążenia. Standard definiuje osiem poziomów priorytetów w odniesieniu do ruchu asynchronicznego. W trybie asynchronicznym realizowany jest zwykle przekaz danych. Każdej stacji przydzielony jest czas na transmisję ramek synchronicznych. Gdy czas ten nie jest w pełni wykorzystany, stacja może transmitować zgromadzone przez nią ramki asynchroniczne.

Ramki są transmitowane jedynie przez stację będącą posiadaczem tokena. Każda stacja dołączona do pętli podstawowej (pętle tworzy ciąg połączeń typu punkt-punkt) dokonuje analizy i regeneracji ramki (z wyjątkiem stacji uszkodzonych, wyłączenych z pętli). Stacja będąca adresatem ramki kopiuje jej zawartość do

bufora wewnętrznego. Podobnie jak w IEEE 802.5 ramka jest usuwana z pętli przez stację źródłową, która jest też odpowiedzialna za umieszczenie wolnego tokena w kanale wyjściowym.



Rys. 4.73. Zależność pomiędzy czasem TRT obiegu tokena, obciążeniem pętli i priorytetami obsługiwanej ruchu

Standard FDDI opisuje mechanizm czasowego tokenowego sterowania dostępem do medium, który pozwala stacji źródłowej danej wiadomości na określenie jej priorytetu i realizację kolejnych faz procesu transmisji. Każda stacja dokonuje na bieżąco pomiaru czasu TRT obiegu tokena i porównuje ten czas z nominalnym czasem TTRT obiegu tokena. Jeżeli  $\text{TRT} < \text{TTRT}$ , wówczas stacja może przesyłać wszystkie zgromadzone przez nią ramki obsługiwane jako synchroniczne (w ramach przyznanego jej limitu  $SA_i$ , a przez tzw. czas THT (ang. *Token Holding Time*) posiadania tokena;  $THT = TTRT - TRT$ , pozostałe ramki asynchroniczne o niższym priorytecie. Przy wzroście obciążenia medium może dojść do sytuacji, gdy czas TRT będzie większy od TTRT. Przekroczenie czasu TTRT jest wówczas sygnalizowane w stacji zmianą stanu (flagi) specjalnego licznika LC spójnionych tokenów. Gdy czas obiegu tokena rośnie, tzn.  $\text{TRT} > \text{TTRT}$ , a  $LC=1$  wówczas jedynie wiadomości o najwyższym priorytecie (ramki synchroniczne) mogą być transmitowane po uprzednim przechwyceniu tokena.

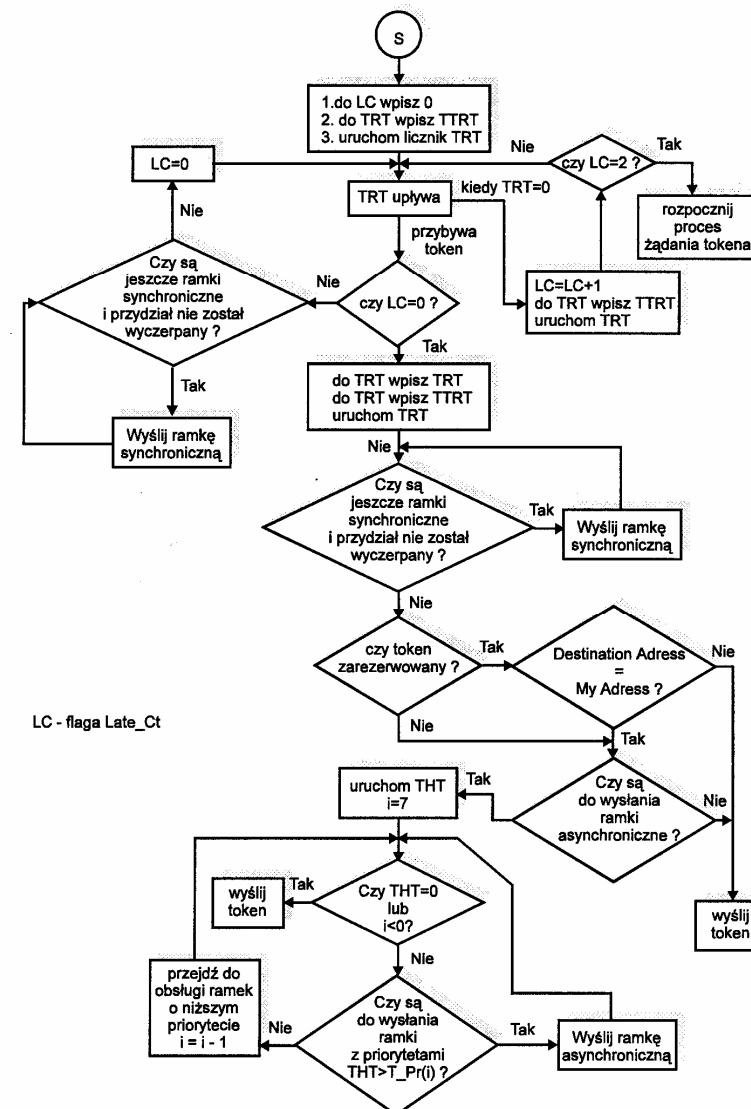
Zgodnie z ilustracją podaną na rysunku 4.73 obciążenie pętli jest proporcjonalne do czasu obiegu tokena TRT. Jeszcze raz należy podkreślić fakt, że **transmisja ramek asynchronicznych może mieć miejsce wtedy i tylko wtedy, gdy po przechwyceniu tokena mamy  $LC=0$** . Początkowe wartości parametrów dla każdej stacji to  $TRT = TTRT$  i  $LC = 0$ . Każdorazowo po odbiorze tokena wartość licznika TRT jest ustawiana na TTRT. Wartość ta maleje z upływem czasu. Kiedy token napływa przed wyzerowaniem się licznika TRT wartość tego licznika jest ponownie ustawiana jako TTRT, a taki token nazywamy „wczesnym”. W przypadku, kiedy TRT osiągnie 0, a token jeszcze nie przybył, wartość flagi LC zwiększana jest o 1, TRT ponownie przyjmuje wartość TTRT i zaczyna z powrotem maleć. Jeżeli TRT po raz drugi osiągnie 0, stan LC zwiększony jest do 2, a token uważany jest za zagubiony. Następuje zainicjowanie procesu żądania tokena (ang. *claim process*).

W przypadku przybycia tokena „wczesnego” podejmowane są następujące kroki:

1. aktualna wartość TRT jest przepisywana do licznika THT,
2. TRT powraca do wartości TTRT,
3. zaczynamy odmierzać TRT,
4. stacja rozpoczyna nadawanie ramek synchronicznych (przez czas SA),
5. po zakończeniu transmisji ramek synchronicznych uruchamiany jest zegar THT, a wartość THT zaczyna maleć; Stacja może inicjować transmisje ramek asynchronicznych dopóki  $THT > 0$ .

W przypadku przybycia tokena „późnego” (token nazywamy „późnym”, jeśli w chwili jego przybycia  $LC = 1$ ), flaga LC jest ponownie zerowana, natomiast czas TRT nadal maleje. Stacja może wówczas nadać tylko ramki synchroniczne.

Jak wspomniano wcześniej, dla danego systemu FDDI definiowany jest każdorazowo pewien czas obiegu tokena nazywamy nominalnym czasem TTRT, powyżej którego realizowane są jedynie transmisje synchroniczne (np. mowa). **W normalnie funkcjonującym systemie czas obiegu TRT nie może przekraczać wartości  $2TTRT$** , pozwalając tym samym na obsługę stacji pracujących w trybie synchronicznym. **Pamięci lokalne stacji projektowane są tak by ich pojemności gwarantowały możliwość buforowania danych, wymagających obsługi synchronicznej, przez czas nie dłuższy, niż  $2TTRT$** . Natomiast zgłoszenia asynchroniczne o różnych priorytetach obsługiwane są jedynie wtedy, gdy pomierzony przez stację czas TRT jest mniejszy od TTRT. W przypadku, gdy czas obiegu tokena TRT przekroczy  $2TTRT$ , sygnalizowana jest niesprawność pętli. Flaga LC przyjmuje wówczas wartość 2, powodując zainicjowanie procedury wykrywania nieprawidłowości w pracy sieci. Procedura ta wymaga, by każda stacja przesyłała ramkę typu CLAIM TOKEN (żądanie tokena) z wartością czasu TTRT wymaganą przez tę stację do obsługi jej ruchu synchronicznego. Stacją zwycięską, tj. przejmującą token, staje się ta, która zadeklarowała najmniejszą wartość TTRT. W przypadku identycznych wartości czasów nominalnych TRT posiadaczem tokena staje się stacja o największym adresie.



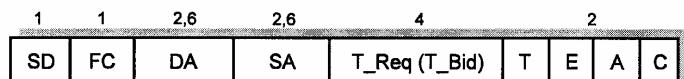
Rys. 4.74. Algorytm sposobu przydziału dostępu do medium

**Zgłoszenia asynchroniczne są podzielone na 8 klas priorytetów (poziomów).** Dla każdego poziomu ustawiany jest czas  $T_{Pr(i)}$  - określający maksymalny czas

nadawania ramek danego poziomu. Stacja może nadawać informacje z poziomu "i" dopóki  $THT > T_{Pr(i)}$ . Maksymalna wartość  $T_{Pr(i)}$  nie może być większa niż TTRT. Schemat ten oparty jest na standardzie IEEE 802.4. Sieć działań dla algorytmu przydziału dostępu do medium przedstawiono na rysunku 4.74.

#### 4.2.8.9 Proces żądania tokena (claim process)

**Protokół FDDI definiuje szereg procedur utrzymywanych. Jedną z podstawowych procedur jest proces żądania tokena.** Proces ten realizowany jest w podwarstwie MAC. Postać formatu ramki w procesie żądania tokena przedstawiono na rysunku 4.75. Proces żądania tokena uruchamiany jest w momencie włączenia nowej stacji lub w momencie wykrycia błędów w działaniu zarówno stacji jak i łączy fizycznych. Nadzór nad jakością i sprawnością połączeń fizycznych jest częścią funkcji zarządzających. Obiekt MAC może być umieszczony w pierścieniu tylko w przypadku połączenia właściwych portów, zapewnienia dobrej jakości łącza i prawidłowego kodowania.



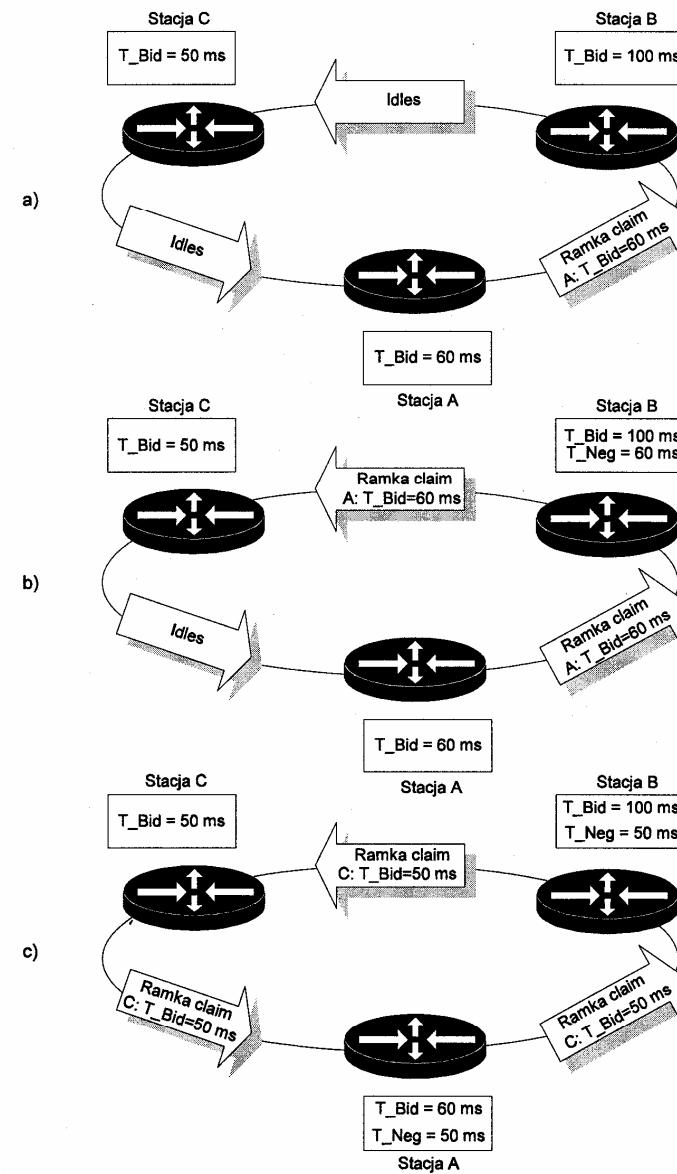
- FC - pole to stanowią ciągi o specjalnej strukturze odmiennej dla adresów 48-bitowych i 16-bitowych
- DA, SA - DA = SA
- $T_{Req}$  - żądany czas TTRT
- E - wakaźnik błędu; musi być ustawiony na R aby ramka była ważna
- A, C - wskaźniki, które nie powinny być ustawiane przez żadną stację

Rys. 4.75. Format ramki FDDI w procesie żądania tokena

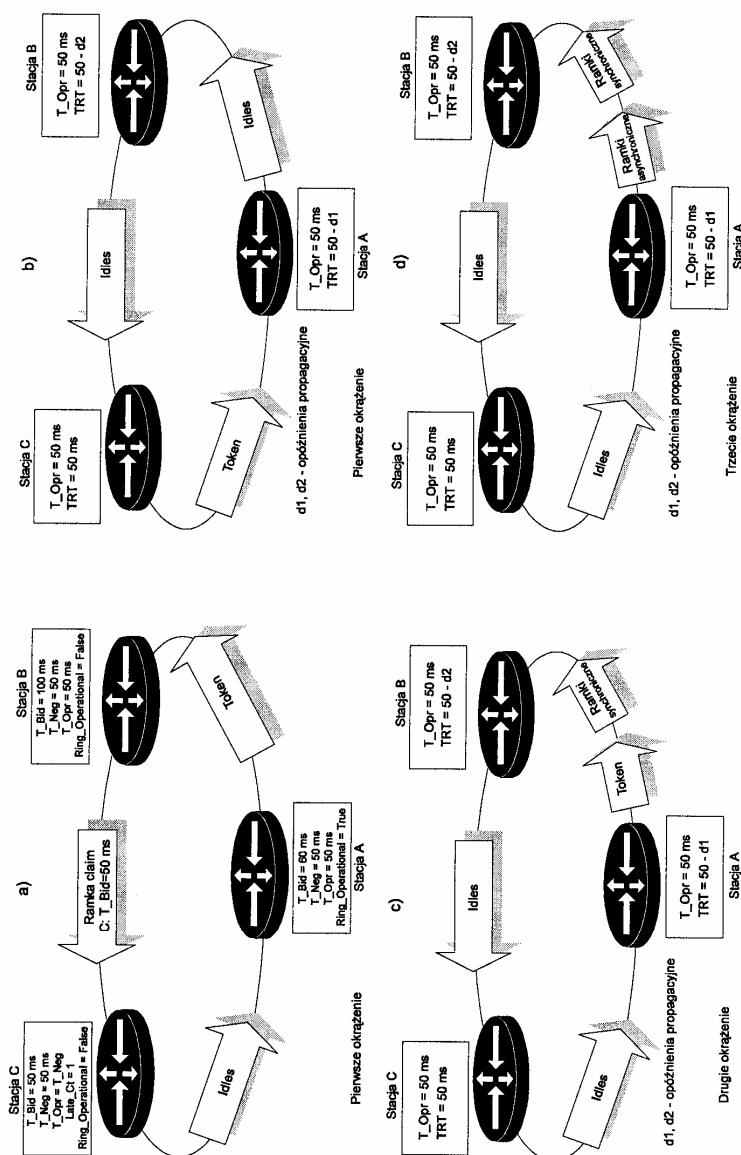
W procesie żądania tokena poszczególne stacje rywalizują o prawo inicjacji pierścienia przez ciągłe nadawanie ramek żądania tokena.

Każda stacja porównuje napływaną wartością  $T_{Bid}$  ( $T_{Bid}$  stanowi wartość  $T_{Req}$  zgłoszaną do „licytacji”) z czasem deklarowanym przez siebie i podejmuje odpowiednie działania:

- gdy  $T_{Bid}$  przychodzące  $> T_{Bid}$  własnego - do ramki wstawiana jest wartość  $T_{Bid}$  własnego;
- gdy  $T_{Bid}$  przychodzące  $< T_{Bid}$  własnego - przepuszczanie ramek przychodzących;
- gdy  $T_{Bid}$  przychodzące  $= T_{Bid}$  własne - w tym przypadku rozstrzygnięcie następuje wg. poniższych zasad :
  - ramka z najniższym czasem TTRT ma pierwszeństwo;
  - kiedy TTRT są takie same, ramka z adresem 48-bitowym ma pierwszeństwo;
  - kiedy TTRT i adresy są takie same, ramka z większym adresem ma pierwszeństwo.



Rys. 4.76. Kolejne etapy licytacji



Rys. 4.77. Ilustracja kolejnych etapów inicjacji w procesie żądania tokena

#### 4.2.8 FDDI - Protokół dostępu do medium światłowodowego

Proces uważa się za zakończony, gdy stacja odbierze z pętli wysłaną przez siebie ramkę. Z drugiej strony proces musi się zakończyć w ograniczonym czasie. Do licznika TRT przepisywana jest wartość  $T_{Max}$ . Jeśli TRT upłynie, a proces żądania nie zakończy się, konieczne jest uruchomienie procesu beacon.

Proces żądania tokena składa się zatem z dwóch części :

- licytacji - na tym etapie wszystkie stacje ustalają wartość TTRT oraz
- inicjowania - jedna stacja uzyskuje prawo do wysłania tokena. Pozostałe ustawiają swoje zmienne i liczniki na odpowiednie wartości.

Kolejne fazy procesu licytacji zilustrowano na rysunku 4.76, a kolejne fazy procesu inicjalizacji przedstawiono na rysunku 4.77.

#### Licytacja czasu obsługi w procesie żądania tokena

Przyjmijmy, że stacją uruchamiającą proces jest stacja A. Każda ze stacji uczestniczących w procesie ma ustaloną wartość zmiennej  $T_Bid$ , którą licytuje. Podczas procesu żądania tokena do licznika TRT wpisywana jest wartość zmiennej  $T_{Max}$  (165 ms).

Stacja A rozpoczyna proces (patrz rysunek 4.76a), wysyłając ramkę z przykładową wartością  $T_Bid = 60 \text{ ms}$ . Stacje B i C znajdują się w stanach T0 (oznacza to: przesyłaj symbole Idle) i R0 (oznacza to: powtarzaj przychodzące dane). W zależności od zawartości napływających ramek stany te mogą ulegać zmianom.

Stacja B (rysunek 4.76b) dokonuje następujących czynności:

- sprawdza czy ramka operuje na adresach 48-mio bitowych,
- porównuje pole DA ze swoim adresem; w tym przypadku pola te nie są zgodne,
- porównuje pole SA za swoim adresem i ustawia flagę H\_Flag, jeśli adres przychodzącej ramki jest większy, w przeciwnym przypadku ustawia flagę L\_Flag,
- porównuje wartość  $T_Bid = 60 \text{ ms}$  ze swoją deklarowaną wartością  $T_Bid$  równą 100 ms. Stacja żąda większego czasu, co nie może zostać spełnione. Ustawia flagę H\_Flag,
- flaga Higher\_Claim nakazuje nadanie otrzymanej ramki; ostatecznie stacja B ustawia  $T_Neg = T_Bid\_Received$ .

Kolejne czynności podejmowane przez stację C (patrz rysunek 4.76c) są takie same jak w stacji B z następującą różnicą :

- stacja C zauważa, że jej własne  $T_Bid$  jest mniejsze od otrzymanego ( $T_Bid\_Received$ ). Poprzez ustawienie odpowiednich wskaźników ( $L\_Flag$  i  $Lower\_Claim$ ) nakazuje nadajnikowi i odbiornikowi przechwycenie ramki pochodzącej z stacji A i wysłanie własnej.

Po obiegu całej pętli ramka powtórnie dociera do stacji A, która stwierdza, że nie może już nadawać ramek z wyższą wartością  $T_Bid$ . Przepuszcza więc ramkę ze stacji C, ustawiając jednocześnie  $T_Neg = 50 \text{ ms}$ .

Stacja B zmienia T\_Neg z 60 ms na 50 ms.

Dochodzimy do sytuacji jak na rysunku 4.76c, kiedy to stacja C otrzymuje „swoją” ramkę. Automatycznie ustawiana jest flaga My\_Claim, informująca nadajnik o zaprzestaniu nadawania ramek. Liczniki i flagi ustawiane są następująco T\_Opr = T\_Neg, TRT = T\_Opr, Late\_Ct = 1 i Ring\_Operational = False.

Nadany zostaje token.

Zmienna logiczna Ring\_Operational - wskazująca stan pierścienia - ustawiana jest na wartość False w momencie rozpoczęcia procesu żądania tokena: oznacza to, że nie może wówczas zostać nadana żadna ramka z danymi.

#### Faza inicjacji w procesie żądania tokena

Rysunek 4.77a pokazuje stan sieci po zakończeniu procesu żądania tokena. W wyniku tego procesu stacja C wysyła token. Kolejne stacje ustawiają liczniki i flagi ( $T_{Opr} = T_{Neg}$ ,  $Late_{Ct} = 1$ ,  $Ring_{Operational} = True$ ) nie nadając przy tym żadnych ramek.

Stacja C otrzymuje swoje, napływające z opóźnieniem, kolejne ramki żądania tokena. Nie mają one już jednak znaczenia, gdyż poprzedni proces został zakończony. Gdyby w tym momencie napłynęła ramka pochodząca od innej stacji, to proces żądania tokena rozpocząłby się od początku. Taka sytuacja mogłaby mieć miejsce, gdyby w chwili wygrania żądania tokena przez stację C, do pierścienia włączły się nowa stacja.

Kiedy stacja C odbiera wysłany przez siebie token, ustawia flagę  $Ring_{Operational} = True$ . Nie może jednak nadawać żadnych ramek, gdyż w momencie otrzymania tokena zmienna logiczna miała wartość  $Ring_{Operational} = False$  (rysunek 4.77b).

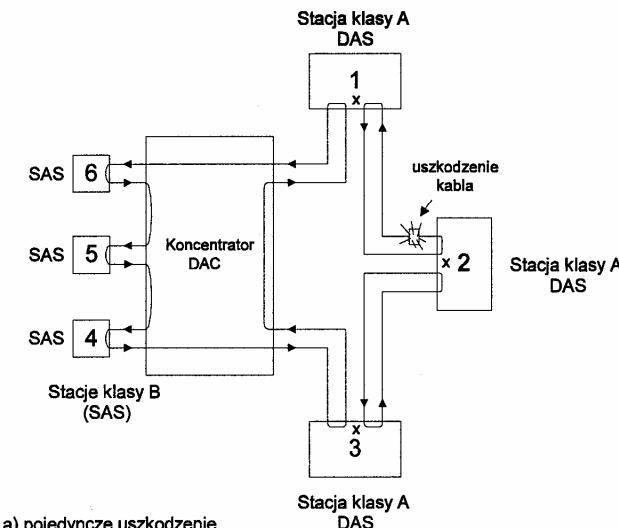
Stacja A przechwytuje token, ustawia licznik  $Late_{Ct} = 0$  i rozpoczyna nadawanie ramek synchroniczne. Nie może jednakże nadawać ramek asynchronicznych, gdyż w momencie otrzymania tokena licznik  $Late_{Ct}$  był ustawiany na wartość 1 (patrz rysunek 4.77c).

W kolejnej fazie algorytmu stacja C otrzymuje w końcu szansę na nadanie ramek synchronicznych. Z kolei stacja A może już nadawać również i ramki asynchroniczne (rys. 4.77d).

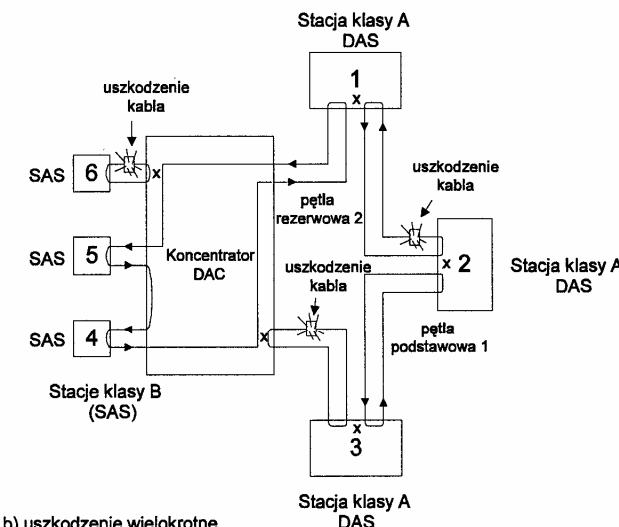
#### 4.2.8.10 Proces nawiązywania połączeń w przypadku awarii łącza lub stacji

Jeśli proces żądania tokena nie zakończy się przed upływem czasu  $T_{Max}$ , oznacza to, że mogło nastąpić przerwanie pętli. Stacja, która jako pierwsza wykryje taki stan, zaczyna nadawać ramki sygnalizacyjne (ang. *beacon frames*). Proces kończy się, gdy stacja otrzyma ponownie swoje ramki. W przeciwnym przypadku, po ok. 370 ms uruchamiana jest funkcja śledzenia pracy pierścienia (dokładniejsze informacje na ten temat zawarte są w części dotyczącej utrzymywania pętli) powodująca testowanie wszystkich stacji. Stacje działające wadliwie

są usuwane z pierścienia, następuje jego rekonfiguracja i uruchomiony zostaje proces żądania tokena.

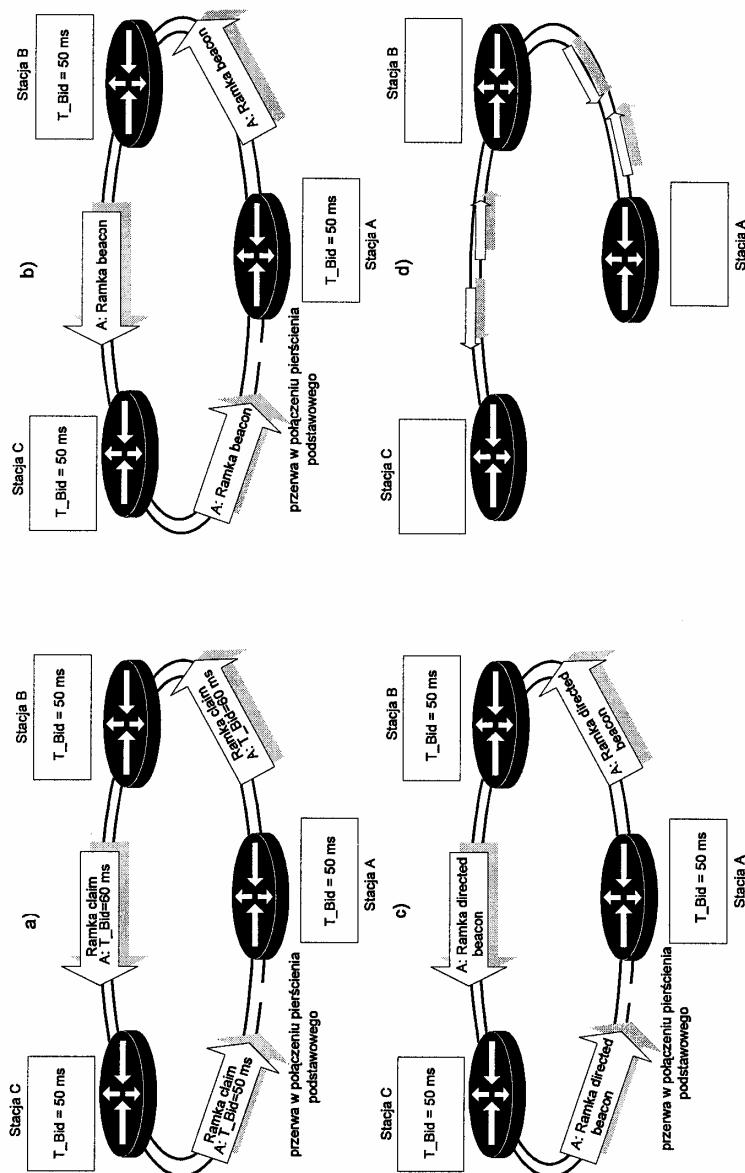


a) pojedyncze uszkodzenie



b) uszkodzenie wielokrotne

Rys. 4.78. Przykłady rekonfiguracji pętli FDDI w przypadku jej uszkodzeń:  
a) uszkodzenie pojedyncze, b) uszkodzenie wielokrotne



Rys. 4.79. Ilustracja procesu nawiązywania połączenia w przypadku awarii łącza lub stacji

W przypadku przekroczenia limitu czasu 2TTRT, co może wiązać się np. z przerwą w pętli, stacje transmitują ramki typu beacon, które są sukcesywnie retransmitowane. Analiza adresów stacji źródłowych tych ramek pozwala na lokalizację uszkodzenia i rekonfigurację pętli. Brak zasilania stacji powoduje jej automatyczne odłączenie. Uszkodzenie lub niesprawność łącza światłowodowego w konfiguracji dwukanałowej powoduje rekonfigurację systemu do postaci jednokanałowej. Procedury zarządzania pracą stacji pozwalają na automatyczne przywrócenie połącznej pętli, gdy tylko uszkodzenie zostaje naprawione. Przykłady rekonfiguracji sieci FDDI w przypadku pojedynczych lub wielokrotnych uszkodzeń ilustruje rysunek 4.78.

Kolejne etapy procesu nawiązywania połączeń w przypadku awarii łącza przedstawiono na rysunku 4.79. W pierwszym okresie wystąpienia "niezidentyfikowanego" jeszcze uszkodzenia łącza transmisyjnego wszystkie stacje nadają ramki żądania tokena (patrz rysunek 4.79a). Po upływie czasu  $T_{Max}$ , stacja A zauważa nieprawidłową pracę pierścienia (nie otrzymuje żadnych ramek). Stacja A rozpoczyna więc nieprzerwane wysyłanie ramek beacon, czekając na odbiór jakiegoś ramki tego typu (rysunek 4.79b). Jeżeli w stacji A upłynął czas  $T_{Stuck} = 8$  ms, to stanowi to sygnał dla procedury RM (ang. *Ring Monitoring* - jedna z procedur zarządzania) do rozpoczęcia nadawania ramek typu directed beacon. Informują one stację zarządzającą, że w pierścieniu wystąpiła przerwa spowodowana błędem stacji lub uszkodzeniem łącza (rysunek 4.79c). Stacja A wysyła ramki typu directed beacon przez czas  $T_{Direct} = 370$  ms. Jeżeli nie otrzyma ona w tym okresie swojej ramki uruchamia proces śledzenia stanu stacji, wykrywający każde uszkodzenie w układach odbiornika lub nadajnika. Następnie rekonfiguracja pierścienia, mająca na celu wyeliminowanie błędnej stacji (rysunek 4.79d).

#### 4.2.8.11 Zarządzanie siecią FDDI

FDDI jest przykładem sieci z wbudowanymi funkcjami zarządzającymi zarówno na poziomie lokalnym jak i globalnym. W rozdziale tym zaprezentujemy strukturę i sposób działania podwarstwy SMT.

Organizacja bloku zarządzania SMT (ang. *Station Management*) i funkcje zarządzania siecią

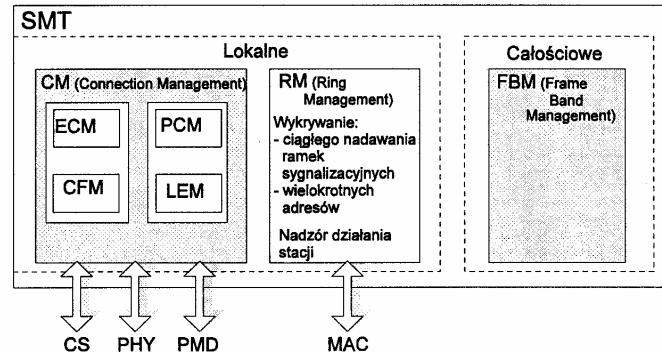
SMT podzielić można na dwie części (patrz rysunek 4.80). Są to:

- **zarządzanie na poziomie lokalnym** - dotyczy ono
  1. pojedynczej stacji i ma na celu usuwanie i dodawanie stacji do pierścienia, jej inicjację i konfigurację, izolację pojedynczej stacji oraz zbieranie statystyk  
bądź
  2. połączenia - obejmując zarządzanie połączeniami, monitorowanie, wykrywanie błędów, zbieranie statystyk

oraz

- zarządzanie zdalne całą siecią**

W tym przypadku administrator sieci musi mieć możliwość zdalonego monitorowania i konfigurowania pojedynczych stacji i połączeń, tak aby w porę zareagować na problemy pojawiające się w różnych częściach sieci.



Rys. 4.80. Organizacja bloku SMT

Przedstawionym powyżej poziomom - lokalnemu i globalnemu - zarządzania odpowiadają ściśle określone funkcje.

- Poziom połączenia - LLM (ang. Link Level Management).**

Procesy tego poziomu odpowiedzialne są za zapewnienie niskiej stopy błędów. W tym celu nadzorują one prawidłowość połączeń portów i monitorują realizowane połączenia. Zbierane są również dane statystyczne dotyczące tych połączeń. W skład LLM wchodzą trzy procesy omówione w dalszej części: PCM (ang. Physical Connection Management), CFM (ang. Configuration Management) i LEM (ang. Link Error Monitoring).

- Poziom stacji - NLM (ang. Node Level Management)**

Procesy tego poziomu odpowiedzialne są za włączanie i usuwanie stacji do i z pierścienia, jej inicjację i konfigurację, izolują także stację w momencie wykrycia błędów. Na tym poziomie kontrolowane jest działanie optycznych układów obejściowych. Zbierane są również dane statystyczne dotyczące działania stacji. W skład NLM wchodzą dwa procesy omówione w dalszej części: ECM (Entity Coordination Management) i CFM (Configuration Management).

- Poziom całej sieci - NLM (ang. Network Level Management)**

Ta część SMT odpowiedzialna jest za kontrolę działania układów podwarstwy MAC, mianowicie: wykrywanie wielokrotnych adresów, wykrywanie i likwidację ciągłego nadawania ramek sygnalizacyjnych, testowanie stacji. Protokoły NLM umożliwiają zdalne

#### 4.2.8 FDDI - Protokół dostępu do medium światłowodowego

zarządzanie siecią, wykorzystując do tego celu specjalizowane bazy danych MIB (ang. *Management Information Base*). W skład NLM wchodzą: RMT (ang. *Ring Management*) i FBMT (ang. *Frame Based Management*)

##### Nadzorowanie połączeń i zarządzanie pracą pętli

Procesy nadzorowania połączeń i utrzymania pętli są realizowane w oparciu o zestaw wymienionych poniżej procedur:

###### 1. Zarządzanie połączonymi (ang. CM - *Connection Management*)

Zarządzanie połączonymi obejmuje szereg procedur. Są to między innymi:

- Zarządzanie pracą obiektów ECM (ang. Entity Coordination Management).**

Procedura ta odpowiada za działanie wszystkich portów i za optyczne układy obejściowe znajdujące się w danej stacji. Testuje ona też wewnętrzne połączenia pomiędzy portami, a obiektami podwarstwy MAC.

- Zarządzanie konfiguracją CFM (ang. Configuration Management).**

Jak wiadomo, standard FDDI definiuje dwa pierścienie: podstawowy i dodatkowy. Wewnątrz stacji pierścień te nazywane są odpowiednio: ścieżką podstawową i ścieżką dodatkową. CFM zarządza tymi ścieżkami podłączając je do odpowiednich pierścieni lub tworząc ścieżki lokalne używane w celach diagnostycznych. Koncentratory FDDI posiadają przełączniki (komutatory) CS umożliwiające odłączenie wybranych lub wszystkich stacji podłączonych do pierścienia. Nadzór nad działaniem przełącznika sprawuje CFM.

- Zarządzanie połączonymi PCM (ang. Physical Connection Management).**

Procesy wchodzące w skład PCM identyfikują właściwe połączenia portów, usuwają nielegalne topologie (np. dodatkowy pierścień), rozpoznają stacje uczestniczące w połączeniu (użyteczne w aplikacjach, gdzie tylko jedna stacja ma prawo nadawania). Zapewniają właściwą synchronizację połączenia i czuwają nad minimalną wartością stopy błędu. Aby procesy PCM zostały uaktywnione, spełnione muszą być dwa warunki:

- musi istnieć fizyczne połączenie między stacjami;
- odbiorca musi być aktywny, a jego PCM działać poprawnie.

- Utrzymanie połączzeń LEM (ang. Link Error Monitoring).**

Odpowiada za testowanie połączenia (ciągłe lub okresowe) z wykorzystaniem jednej z poniższych metod:

- nadajemy symbole Idle i liczymy błędy w strumieniu przychodzącym,
- nadajemy jednostki danych PDU (ang. *Protocol Data Unit*) i liczymy błędy strumieniu przychodzącym,
- nadajemy jednostki danych PDU i sprawdzamy pola FCS ramek,

- nadajemy ciąg symboli i w strumieniu przychodząym liczymy błędy; odbiorca retransmituje dokładnie to, co otrzymał.

## 2. Utrzymanie pętli (ang. RM - Ring Management)

RM kontroluje operacje wykonywane przez obiekty podwarstwy MAC. W stacjach z wieloma obiektami obowiązuje przy tym zależność, że na jeden obiekt MAC przypada jeden element RM. Do zadań RM należą między innymi:

- Wykrywanie ramek sygnalizacyjnych (ang. *beacon frames*).

Stacje biorące udział w procesie nawiązywania połączeń w przypadku awarii łącznej lub stacji mogą nieprzerwanie nadawać ramki sygnalizacyjne. Ma to miejsce w sytuacji wadliwie działającego układu scalonego odpowiedzialnego za funkcje podwarstwy MAC lub pojawienia się błędów wewnętrznych stacji, np. uszkodzenia ścieżki. RM wykrywa te stany i po czasie nadawania ramek sygnalizacyjnych ( $T_{Stuck} = 8$  ms) wysyła ramki rozgłoszeniowe informujące pozostałe stacje i administratora o blokadzie jednej z nich (ramki nadawane są przez czas  $T_{Direct} = 370$  ms). Jeśli w dalszym ciągu dana stacja nie otrzymuje swoich ramek, uruchomiona zostaje funkcja śledzenia pracy stacji.

- Śledzenie pracy stacji (ang. *trace function*).

W momencie wykrycia ciągłego nadawania ramek sygnalizacyjnych przez wadliwie działającąację stację, uruchamiany jest test połączeń. Ma on za zadanie zbadanie struktur wewnętrznych stacji. Jeżeli stacja poprawnie przejdzie test, jest ona ponownie uruchamiana i testowana przez procesy CM. Jeżeli wykryte zostaną błędy w działaniu stacji, jest ona wyłącza, a pierścień - rekonfigurowany.

- Wykrywanie identycznych adresów.

Jeżeli dwa lub więcej obiektów MAC ma ten sam adres, pętla nie może działać poprawnie. Istnienie wielokrotnych adresów wykrywane jest w następujących przypadkach:

- Stacja otrzymuje własne ramki sygnalizacyjne, a wysyła ramki żądania tokena (ang. *claim frames*) przez czas dłuższy niż maksymalne opóźnienie pierścienia FDDI ( $D_{Max}$ ). Oznacza to, że inna stacja o tym samym adresie wysyła ramki sygnalizacyjne.
- Stacja otrzymuje "własne" ramki żądania tokena, podczas gdy wysyła ramki sygnalizacyjne przez czas dłuższy niż  $D_{Max}$ .
- Stacja otrzymuje własne ramki żądania tokena przez czas większy niż  $D_{Max}$ , po tym jak wygrała proces żądania.
- Stacja otrzymała własną ramkę żądania tokena z inną wartością TTRT.

W momencie wykrycia istnienia stacji ze zduplikowanym adresem należy uniemożliwić realizację usług przez podwarstwę LLC, aby uniknąć problemów z protokołami warstw wyższych. Następnie można zastosować jedno z rozwiązań:

- Zmienić adres - metoda ta wymaga posiadania przez stację kilku przydzielonych adresów 48-bitowych lub 16-bitowych. Przed zmianą adresu należy usunąć wszystkie PDU wysłane ze zduplikowanym adresem. Zaleca się, by wszystkie ważne elementy sieci (routery, serwery) posiadały przydzielonych kilka adresów.
- Wysyłać specjalny typ ramek sygnalizacyjnych (*jam beacon frames* z polem *Destination Address = My Long Address*). W tym samym czasie należy przekonfigurować obiekt MAC tak, aby przegrać proces żądania tokena. Ma to na celu uniknięcie pojawienia się w pierścieniu wielu tokenów. Stacje z identycznymi adresami, otrzymując ramki, muszą zmienić adres lub wyłączyć się z pierścienia.
- Stację z powielonymi adresami usunąć z pierścienia.

Z powyższych metod najłatwiejszą, a jednocześnie efektywną jest metoda trzecia. Metody pierwsza i druga stosowane mogą być do stacji mających kluczowe znaczenie dla pracy pierścienia (serwery, routery).

## Zdalne zarządzanie siecią

Zarządzanie globalne pracą sieci realizowane jest z pomocą:

- Bazy danych, w której znajdować się będą informacje o poszczególnych elementach sieci (takich jak mosty, routery, retransmitery). Standard FDDI definiuje taką bazę zwaną **MIB** (ang. *Management Information Base*)
- Protokołu, który byłby w stanie dostarczać wiadomości do i z urządzeń. Bardzo popularnym protokołem jest **SNMP** (*Simple Network Management Protocol*) używany we wszystkich rodzajach sieci. FDDI specyfikuje jednak swój własny protokół zarządzający. Wśród protokołów zarządzających pracą sieci definiowany jest też protokół oparty na normach ISO, zwany **CMIP** (ang. *Common Management Information Protocol*).

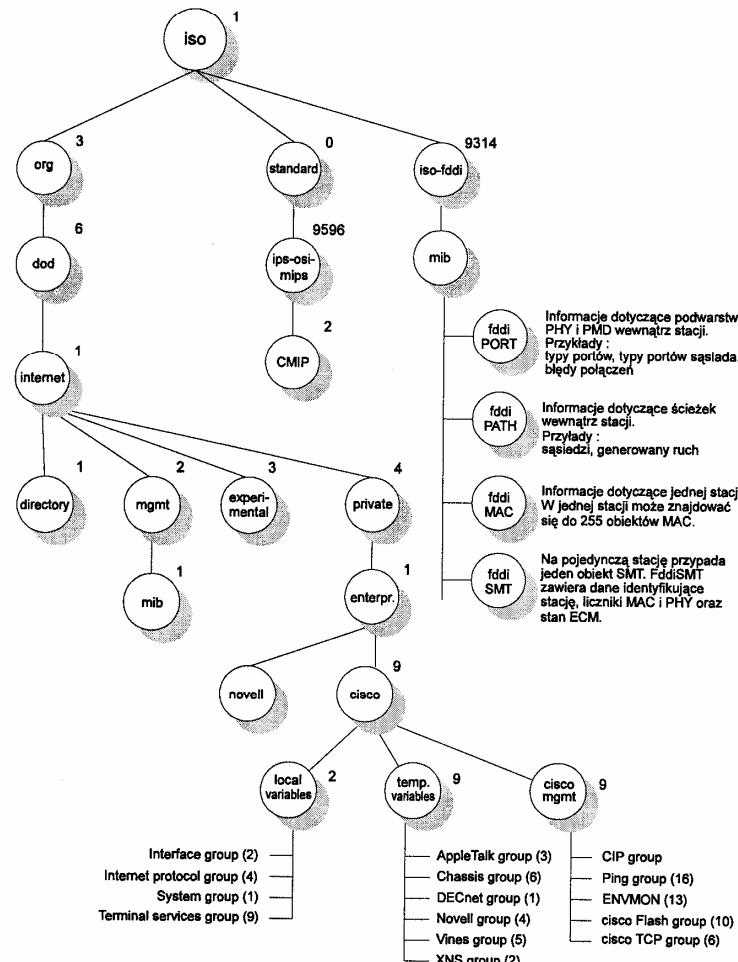
Strukturę samej bazy danych, informacje, które należy lub nie w niej składować oraz sposób wykorzystania tych danych zawiera dokument OSI zwany SMI (ang. *Structure of Management Information*). Opisuje on dokładnie liczbę, typy i atrybuty obiektów dla wielu sieci (FDDI, Ethernet, itp.), definiuje strukturę, podstawowe operacje, właściwości oraz powiązania z innymi atrybutami.

Język programowania użyty do opisu informacji zawartych w MIB to ASN.1 (ang. *Abstract Syntax Notation One*).

Do zarządzania pracą, poza bazą danych, potrzebny jest zbiór zasad określających wymianę danych w całym systemie. Zawarte w nim muszą być informacje o kolejności transmisji bitów, typach danych, długościach danych i wartościach danych. Stosowne opisy zawarte są w dokumentach zwanych BER (ang. *Basic Encoding Rules*).

FDDI SMT definiuje ok. 130 atrybutów w MIB. Niektóre z nich występują na stałe (*fddiSMTStationId*), inne - opcjonalnie (*fddiMAC\_Prim*). Do niektórych można zapisywać i odczytywać dane, a z innych tylko odczytywać. FDDI dopuszcza tworzenie dodatkowych grup atrybutów przez producentów sprzętu.

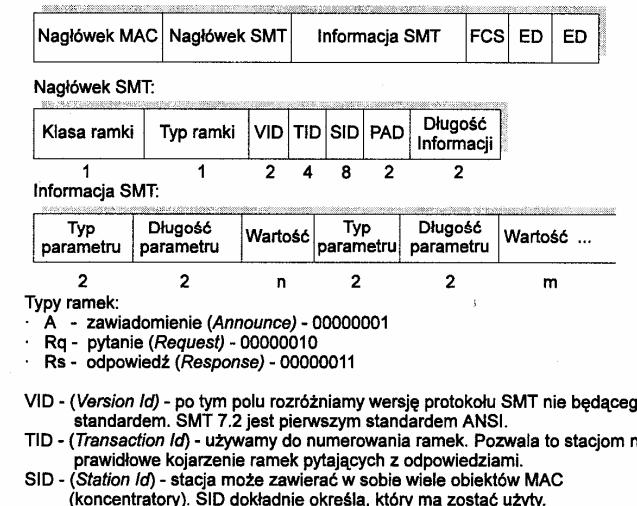
Atrybuty nie mogą pokrywać się z już istniejącymi. Jako przykład posłużyć może MIB stworzony przez firmę Cisco, której produkty stosowane są w kilku akademickich sieciach komputerowych w Polsce. Obiekty występujące w tej bazie zdefiniowane są wg. SNMP SMI, a dostęp do poszczególnych obiektów, grup lub atrybutów odbywa się na zasadach adresów internetowych. Baza danych firmy Cisco w sieci TASK (Trójmiejskiej Akademickiej Sieci Komputerowej) rozpoznawana jest przez identyfikator 1.3.6.1.4.1.9 lub iso.org.dod.internet.private.enterprise.cisco. Poszczególne atrybuty również mają swoje identyfikatory, które „doklejane” są do powyższego adresu, np. zmieniona locIfInBitsSec ma adres 1.3.6.1.4.1.9.2.2.1.1.6.



Rys. 4.81. Sposób kodowania poszczególnych elementów bazy MIB

Sposób kodowania poszczególnych elementów bazy MIB zobrazowano na rysunku 4.81.

Jak już wspomniano, zarządzanie może odbywać się na dwóch płaszczyznach: lokalnej i zdalnej. W pierwszej z nich administrator może ręcznie, przy pomocy klawiatury danej stacji, zmieniać niektóre atrybuty, uruchamiać procesy lub korygować konfigurację. Zarządzanie to ma sens w przypadku sieci małych, skupionych na niewielkim obszarze. W miarę ich wzrostu i pojawiania się środowiska wieloprotokołowego (TCP/IP, NetWare) zarządzanie staje się trudne. Pojawia się konieczność zarządzania siecią z jednej, wydzielonej stacji. FDDI wychodzi temu naprzeciw definiując zbiór ramek zarządzających i sposób ich wymiany. Format ramek SMT przedstawiono na rysunku 4.82. Ramkę SMT rozpoznajemy po wartości pola FC w nagłówku MAC.



Rys. 4.82. Format ramek SMT

**Wymiana tych ramek (SMT PDU) nie wymaga użycia protokołów wyższych warstw**, co pozwala na całosćiowe i jednolite zarządzanie siecią FDDI. W standardzie zdefiniowanych jest 8 klas ramek (tabela 4.10). Wszystkie one mogą być typu zawiadomienia, pytania lub odpowiedzi.

Tabela 4.10. Klasa ramek i sposoby ich kodowania w standardzie FDDI

Klasa ramek	Kod	Typ
NIF (ang. Neighbour Information)	0000	A Rq Rs

Tabela 4.10. Klasy ramek i sposoby ich kodowania w standardzie FDDI (c.d.)

Klasa ramek	Kod	Typ
SIF (ang. <i>Station Information</i> )	0001	Rq
	0011	Rs
ECF (ang. <i>Echo</i> )	0100	Rq Rs
RAF (ang. <i>Resource Allocation</i> )	0101	A Rq Rs
RDF (ang. <i>Request Denied</i> )	0110	Rs
SRF (ang. <i>Status Report</i> )	0111	A
PMF (ang. <i>Parameter Management</i> )	1000 Get	Rq Rs
	1001 Set	Rg Rs
ESF (ang. <i>Extended Service</i> )	1101	A Rq Rs

#### 4.2.8.12 Podwarstwa kanału logicznego LLC

W przypadku sieci FDDI zakłada się, że warstwa łącząca danych oferuje jednolity zestaw usług - oferowanych zgodnie ze standardem ISO 8802.2 (IEEE 802.2).

Pojedynczy obiekt podwarstwy kanału logicznego może obsłużyć wiele punktów udostępniania usług, z których każdy ma adres indywidualny, niepowtarzalny w ramach jednej stacji. Dowolny podzbiór tych punktów (w ramach jednej stacji) może też być adresem grupowym, a wszystkie - adresem rozgłoszania. Takie rozszerzenie jest cenne ze względów użytkowych, umożliwia bowiem świadczenie usług na rzecz wielu różnych obiektów warstwy wyższej, a w przypadku wykorzystania wprost przez procesy użytkowe - obsługę wielu takich procesów.

Warstwa łącząca danych powinna zapewniać możliwość buforowania pakietów zleconych do wysłania. Jeśli podwarstwa dostępu nie gwarantuje tej możliwości, to winna ją realizować podwarstwa kanału logicznego.

Każda jednostka danych warstwy łączącej danych jest przesyłana przy użyciu pojedynczej ramki (jednostki danych protokołu łączącego DL-PDU) identycznej z jednostką danych usług podwarstwy dostępu (MA-SDU = DL-PDU). W normach ISO przyjęto jednolitą postać ramki DL-PDU, w której wyróżnia się cztery pola: pole docelowego punktu udostępniania usług, źródłowego punktu udostępniania usług, typu ramki oraz danych. Pierwsze trzy z tych pól mają długość jednego bajtu, a ostatnie pole jest wielokrotnością bajtu w granicach określonych przez współpracującą z LLC podwarstwę dostępu MAC.

Dla podwarstwy LLC wyróżniane są trzy klasy usług i związane z nim trzy sposoby wymiany informacji między stacjami sieci (omówione w poprzednich paragrafach książki): usługi bezpołączeniowe, usługi połączeniowe i usługi bezpołączeniowe z potwierdzeniami.

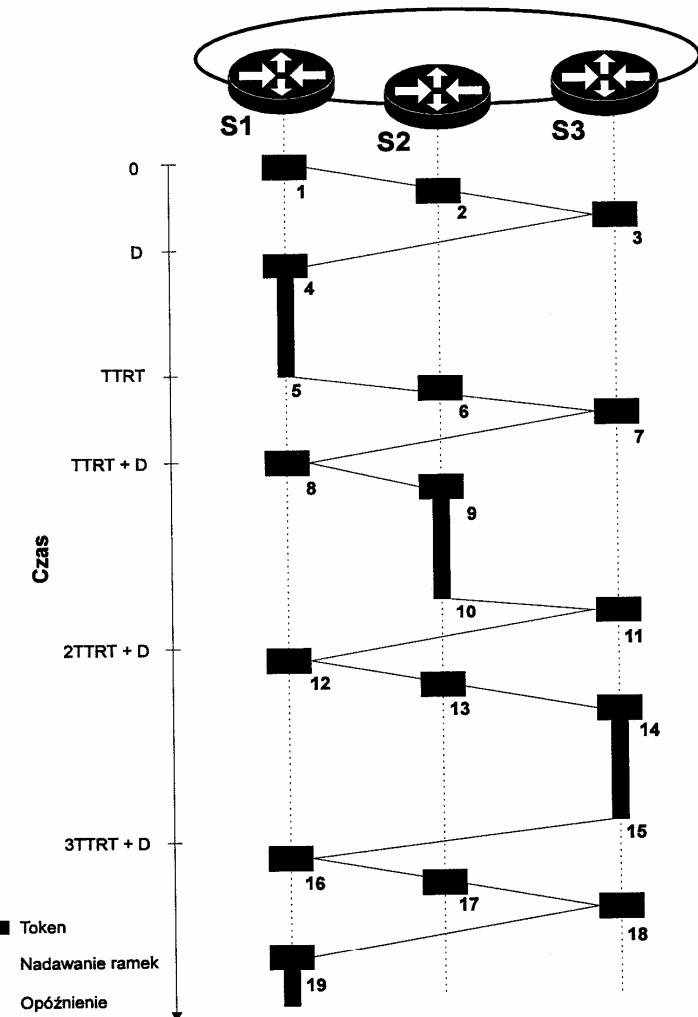
#### 4.2.8.13 Ocena działania sieci FDDI

Parametry mające wpływ na działanie sieci można podzielić m.in. na parametry stałe (nie mogą być kontrolowane przez administratora) i zmienne (np. liczniki). Jakość usług oferowanych przez sieć FDDI może być mierzona efektywnością wykorzystania zasobów sieci. Efektywność czy też wykorzystanie przepustowości sieci jest to stosunek przepustowości pętli wykorzystywanej na efektywne transmisje ramek przez wszystkie stacje, do całkowitej oferowanej przepustowości sieci. Obok efektywności ważny wpływ na jakość oferowanych usług ma opóźnienie dostępu do łączna (okres czasu pomiędzy wyrażeniem gotowości do nadawania, a otrzymaniem tokena). Zależy nam na tym, aby efektywność była jak największa, przy minimalnym czasie oczekiwania na transmisję.

#### Prosty model analityczny

Rozważmy pierścień z 3 stacjami, które po upływie czasu  $t=D$  obiegu tokena wokół pętli chcą nadawać tylko ramki asynchroniczne (patrz rysunek 4.83). Proces transmisji przebiega następująco:

1.  $t = 0$ . Stacja S1 otrzymuje token, ustawia TRT na TTRT, nie ma ramek do nadania, zwalnia token.
2.  $t = t_1$ . Stacja S2 otrzymuje token, ustawia początkową wartość jako TRT = TTRT, przy braku ramek do nadawania zwalnia token.
3.  $t = t_1$ . Stacja S3 otrzymuje token, ustawia TRT = TTRT, przy braku ramek do nadawania zwalnia token.
4.  $t = D$ . Stacja S1 otrzymuje token i nadaje ramki przez czas  $THT=TRT-D$ .
5.  $t = TTRT$ . Licznik THT w stacji S1 wyzerował się, token zostaje zwolniony.
6.  $t = TTRT + t_1$ . Stacja S2 otrzymuje token, nie może jednak nadawać ramek, gdyż licznik TRT wyzerował się. Stacja ustawia TRT = TTRT i zwalnia token.
7.  $t = TTRT + t_1$ . Stacja S3 otrzymuje token, nie może jednak nadawać ramek, gdyż licznik TRT wyzerował się. Stacja ustawia TRT = TTRT i zwalnia token.
8.  $t = TTRT + D$ . Stacja S1 ponownie otrzymuje token, ostatni raz był on w S1 w chwili D, tak więc TRT wynosi zero (TRT mierzony jest od chwili przybycia tokena - 4). Nie można nadawać ramek, następuje zwolnienie tokena.
9.  $t = TTRT + D + t_1$ . Stacja S2 otrzymuje token, licznik TRT zmalał tylko o D, można nadawać ramki przez czas  $THT=TTRT - D$ . Token zostaje zwolniony w chwili  $t = TTRT + D + t_1 + (TTRT - D)$ .



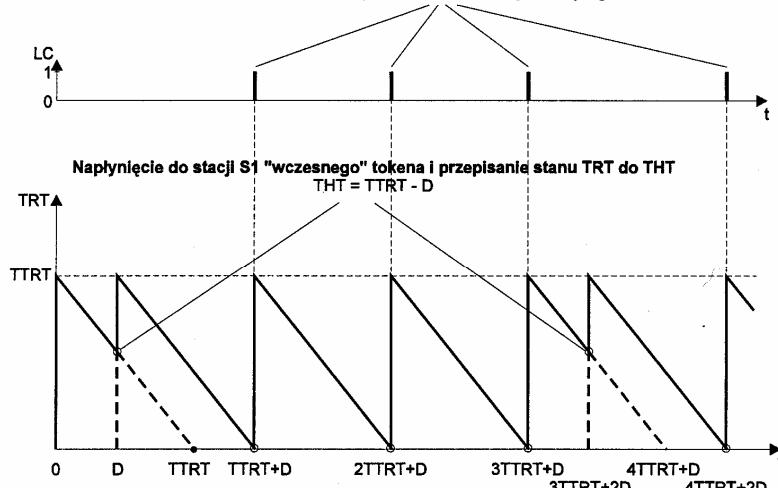
Rys. 4.83. Przydział prawa dostępu do medium dla trzech stacji generujących ramki asynchroniczne

- $t = 2TTRT + t1_2$ . Licznik THT wyzerował się, uwolnienie tokena.
- $t = 2TTRT + t1_3$ . Licznik TRT wynosi zero, przepuszczenie tokena.
- $t = 2TTRT + D$ . Licznik TRT wynosi zero, przepuszczenie tokena.
- $t = 2TTRT + D + t1_2$ . Licznik TRT wynosi zero, przepuszczenie tokena.

- $t = 2TTRT + D + t1_3$ . Stacja S3 otrzymuje token, licznik TRT zmalał tylko o D, można nadawać ramki przez czas  $THT = TTRT - D$ . Token zostaje zwolniony w chwili  $t = 2TTRT + D + t1_3 + (TTRT - D)$ .
- $t = 3TTRT + t1_3$ . Licznik THT wyzerował się, uwolnienie tokena.
- $t = 3TTRT + D$ . Stacja S1 otrzymuje token, kolejne zdarzenia zaczynają się powtarzać.

Wykresy zmian stanów liczników TRT, THT i LC ilustrujące zachowanie się stacji S1 w przypadku obsługi wyłącznie ruchu asynchronicznego ilustruje rysunek 4.84.

Stacja S1  
Napłynięcie tokena do stacji S1 w chwili zerowania się licznika TRT ("późny" token)  
- fakt ten zaznaczono symbolicznie chwilową zmianę flagi z 0 na 1



Rys. 4.84. Wykresy zmian liczników TRT, THT i LC ilustrujące zachowanie się stacji S1 (w przypadku obsługi wyłącznie ruchu asynchronicznego)

### Wnioski

W analizowanym przypadku czas trwania jednego pełnego cyklu pracy stacji sieci wynosi  $3TTRT + D$ . Podczas każdego takiego cyklu, każda stacja nadaje tylko raz przez czas  $TTRT - D$ , a całkowity czas transmisji ramek w sieci wynosi  $3(TTRT - D)$ .

$$\text{Efektywność systemu} = \frac{3(TTRT - D)}{3TTRT + D}$$

Podczas cyklu, po uwolnieniu tokena, każda stacja czeka  $2TTRT + 2D$  na następną okazję do transmisji.

Uogólnienie powyższych rozważań prowadzi do zależności :

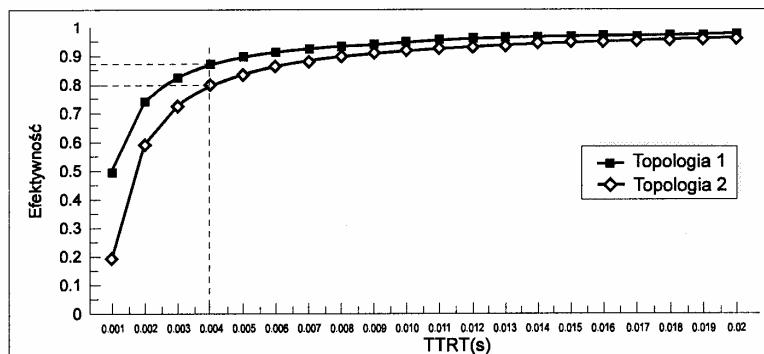
$$\text{Efektywność systemu} = \frac{n(\text{TTRT} - D)}{n\text{TTRT} + D}.$$

Czas oczekiwania na obsługę wynosi więc  $(N - 1)\text{TTRT} + 2D$ ; gdzie N oznacza liczbę stacji w pierścieniu.

#### Optymalny czas TTRT

Najistotniejszy wpływ na efektywność pracy sieci i czas oczekiwania na dostęp do pętli, ma czas TTRT. Na rysunku 4.85 przedstawiono wpływ wartości TTRT na efektywność przy sieci przy założeniu, że jednostkowe opóźnienie propagacyjne światła w światłowodzie wynosi  $5.085 \mu\text{s}/\text{km}$ , a opóźnienie wprowadzane przez stację -  $1 \mu\text{s}$ . Krzywe na rysunku 4.85 zostały wykreślone dla dwóch topologii sieci:

1. topologia 1 zakłada rozpiętość pierścienia 94 km przy 15 aktywnych stacjach (topologia zbliżona do Trójmiejskiej Akademickiej Sieci Komputerowej),
2. topologia 2 zakłada rozpiętość pierścienia 150 km przy 40 aktywnych stacjach.



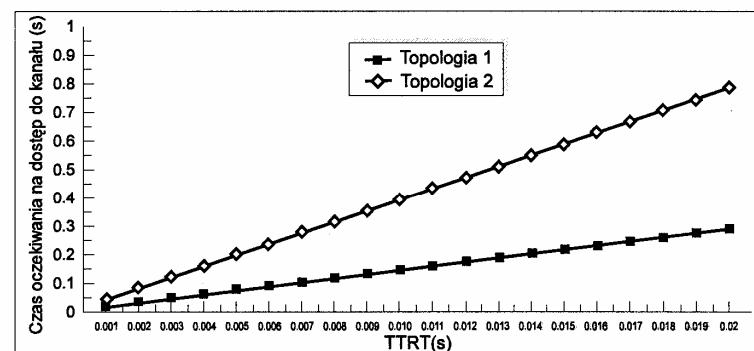
Rys. 4.85. Zależność efektywności od czasu TTRT

Z wykresu 4.86 wynika, że efektywność wzrasta wraz z wartością TTRT. Może to skłonić administratorów do ustalania dużych wartości TTRT. Wiąże się to jednak ze wzrostem czasu oczekiwania na transmisję (patrz rysunek 4.86).

Standard FDDI definiuje minimalną (4 ms) i maksymalną (165 ms) wartość czasu TTRT. W celu osiągnięcia pewnego kompromisu pomiędzy efektywnością, a czasem oczekiwania na transmisję, przyjmuje się zwykle TTRT = 8 ms.

Z rysunków 4.85 i 4.86 odczytać można zależności pomiędzy badanymi wielkościami, a rozmiarami pierścienia. Wraz ze zwiększeniem się rozległości sieci i ze

wzrostem liczby stacji, maleje efektywność wykorzystania sieci. Związane jest to ze wzrostem opóźnień pomiędzy kolejnymi węzłami.



Rys. 4.86. Zależność czasu oczekiwania na transmisję od czasu TTRT

#### 4.2.8.14 FDDI II - propozycja modyfikacji standardu FDDI

*FDDI II jest rozszerzeniem standardu FDDI, dodającym do typowego, asynchronicznego i synchronicznego trybu przekazu pakietów obsługę ruchu izochronicznego.*

W "klasycznym" FDDI nie ma możliwości zestawiania, pomiędzy dwiema komunikującymi się stacjami, połączenia wykorzystującego kanał dedykowany. Nawet ruch synchroniczny, zdefiniowany w standardzie ANSI, nie gwarantuje uzyskania połączenia o stałej przepływności, tak niezbędnej we wszelkich aplikacjach multimedialnych.

*FDDI II posiada klasę usług związanych z zestawianiem połączeń, zapewniających dostęp do medium w ścisłe określonych chwilach i gwarantujących pożądaną przepustowość medium. FDDI II wykorzystuje do tego celu zasadę dostępu zbieżną z metodą określającą mianem pierścienia szczelinowego.* Zasada wirującego pierścienia, wykorzystywana np. w sieci Cambridge Ring, polega na tym, że wokół pętli kraży kilka ramek czasowych (szczelin). Ich rozmiary są ścisłe określone. Stacja, do której dociera pusta ramka, ma prawo wprowadzić do niej stosowne informacje, w tym adres odbiorcy, który po odczytaniu zawartości ramki wprowadza do niej informację potwierdzającą jej odbiór. Po powrocie ramki do nadawcy jej zawartość jest kasowana, a sama ramka czasowa jest ponownie retransmitowana. W metodzie tej istotne są dwa ograniczenia: pierwsze, że nadawać może tylko ta stacja, która odbierze pustą ramkę oraz drugie, że stacji nie wolno dwukrotnie pod rząd zajmować tej samej ramki czasowej. W przypadku, gdy przesyłana ramka ulegnie w procesie transmisji znacznym zniekształceniom, stacja nadawcza może jej nie rozpoznać, a tym samym nie zwolnić szczeliny. Z tego względu jedna ze stacji sieci spełnia funkcję monitora

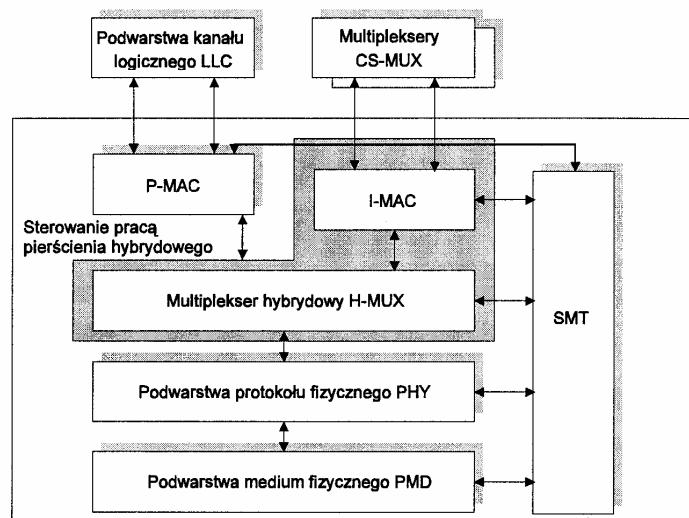
śledzącego wszystkie ramki. Gdy któraś z ramek powtórnie okrąży pierścień, monitor usuwa ją.

W sieci FDDI II co 125 µs generowana jest wieloramka, w której może być wyodrębnionych, zgodnie z techniką TDM, 16 kanałów szerokopasmowych. Nad poprawnym działaniem sieci czuwa stacja monitorująca CM (ang. *Cycle Master*), a przydziałem kanałów czasowych zajmuje się dyspozytor kanałów CA (ang. *Channel Allocator*).

### Architektura FDDI II

Na rysunku 4.87 przedstawiono powiązania pomiędzy poszczególnymi blokami funkcjonalnymi sieci FDDI II. W podwarstwie MAC, w porównaniu ze standarem FDDI, pojawiają się dwa nowe bloki:

- I-MAC (ang. *Isochronous MAC*) - element ten umożliwia izochroniczny dostęp do medium i realizację komutacji kanałów (szczelin czasowych) w trybie połączeniowym.
- HMUX (ang. *Hybrid Multiplexer*) - blok ten jest odpowiedzialny za multipleskowanie dostępu i obsługę zarówno ruchu synchronicznego i asynchronicznego jak też ruchu izochronicznego.



Rys. 4.87. Powiązania pomiędzy blokami funkcjonalnymi FDDI II

Poszczególne rodzaje ruchu zdefiniować można następująco:

1. Ruch asynchroniczny - Wszystkie żądania obsługi rywalizują o dynamicznie przydzielane pasmo (przepustowość medium). Ruch ten generowany jest przez stacje nie wymagające stałego dostępu do medium.

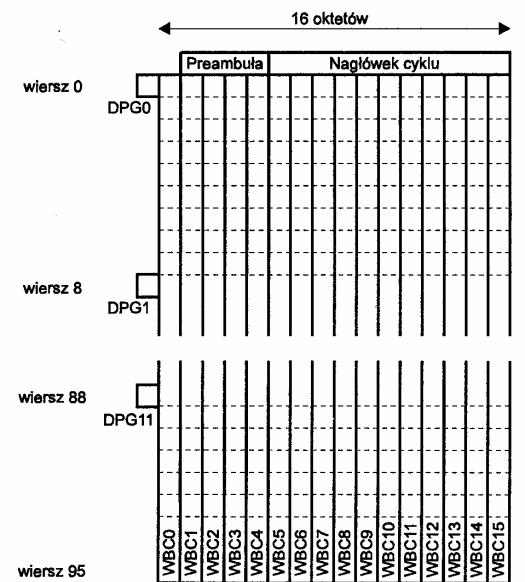
2. Ruch synchroniczny - Każde ze zgłoszeń ma przyznaną wcześniej, pożądaną przepustowość i gwarantowany maksymalny czas opóźnienia w dostępie. Zgodnie z synchronicznym trybem obsługi zgłoszeń przesyłane są np. obrazy.
3. Ruch izochroniczny - W tym przypadku źródło generuje ruch o stałej intensywności. Obsługa ruchu izochronicznego musi gwarantować stały, tj. o wymaganej przepływności dostęp do łączna, niezbędny do przesyłania głosu i obrazu.

Sieć FDDI II zapewnia realizację dwóch zasadniczych trybów pracy:

- podstawowego - udostępniającego typowe usługi bezpołączeniowe standardu FDDI.
- hybrydowego - pozwalającego na pracę zarówno w trybie asynchronicznym, synchronicznym jak i izochronicznym.

Stacje rozpoczynają przy tym pracę w trybie podstawowym, ustawiając odpowiednie liczniki i parametry zgodnie z wymaganiami tego trybu, a następnie, w przypadku pojawiania się zgłoszeń izochronicznych przełączają się w tryb hybrydowy. Dla trybu hybrydowego charakterystyczne jest pojęcie cyklu. Stacja CM (*Cycle Master*), zarządzająca pracą sieci, generuje kolejny cykl (wieloramkę) co 125 µs.

### Format cyklu i definicje kanałów



Rys. 4.88. Struktura pojedynczego cyklu

**Procedura HRC** (ang. *Hybrid Ring Control*) jest protokołem integrującym ruch izochroniczny i asynchronouszny. W celu integracji ruchu wykorzystuje się cykle, w ramach których przenoszone są zarówno zwykłe pakiety (zgłoszenia synchroniczne i asynchronouszne) jak i informacje izochroniczne. Każdy nowy cykl generowany jest przez stację CM co 125 µs. Czas ten został dobrany tak, aby nie było kłopotów z dołączeniem sieci FDDI II do publicznej sieci cyfrowej. Struktura pojedynczego cyklu została pokazana na rysunku 4.88.

W każdym cyklu można wyróżnić 4 zasadnicze elementy:

- **Preambule** - Jest to ciąg 5-ciu symboli (20 bitów) zapewniających właściwą synchronizację pracy pierścienia.
- **Nagłówek cyklu** - Nagłówek definiuje granice cyklu, a także określa sposób wykorzystania poszczególnych, tzw. szerokopasmowych kanałów izochronicznych (patrz rysunek 4.89).

**Poszczególne pola nagłówka mają przy tym następującą interpretację:**

SD - Pole to stanowią symbole J i K (1100010001 - po przekształceniu 4B/5B) definiujące początek cyklu. Ciąg tych symboli, podobnie jak w standardzie FDDI, nie może występować w ciągu danych.

C1 - W tym polu ustawiany jest stan synchronizacji pierścienia. Do tego celu używane są dwa symbole: R lub S. R oznacza, iż synchronizacja nie występuje i każdy cykl może być przerwany przez kolejny, nowy cykl. Symbol S ustawiany jest domyślnie i oznacza pełną synchronizację. Symbol ten ustawiany jest tylko przez stację CM.

W pracy sieci mogą mieć miejsce sytuacje, gdy ramki nie docierają do tej stacji cyklicznie, tj. co 125 µs. Wówczas stacja CM rozpoczyna proces synchronizacji przez ciągłe nadawanie cykli z C1 = R.

Ponowne otrzymanie tego samego cyklu oznacza prawidłowe funkcjonowanie wszystkich stacji. Pozwala to stacji CM nadać cykl z C1=S.

C2 - Pole to informuje o kolejnych numerach cykli. Ustawienie symbolu R oznacza, iż numerowanie nie zostało jeszcze uaktywnione, bądź pojawił się błąd w kolejności cykli. Symbol S oznacza, iż cykle numerowane są prawidłowo, a stacje mogą porównywać pole CS kolejnych ramek.

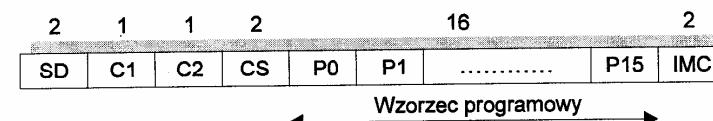
CS - Pole to ma format NN, gdzie N jest symbolem danych. Jeśli w polach C1 i C2 występują symbole R, pole CS interpretowane jest jako pole zawierające pozycję stacji w rankingu stacji monitorujących (wartość od 0 do 63). Pozycja ta używana jest w procesie rywalizacji stacji monitorujących o miano stacji CM.

Podczas normalnej pracy C1 i C2 zawierają symbol S, a pole CS interpretowane jest jako kolejny numer cyklu (od 64 do 255). Stacja CM zwiększa ten numer o 1 przy okazji nadawania nowego cyklu (po wartości 255 następuje 64).

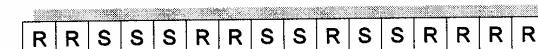
PT (ang. *Programming Template*) - Jest to zbiór 16 pól, każde dla jednego kanału WBC (ang. *Wideband channel*), programujący niejako wykorzystanie

poszczególnych kanałów (stąd nazwa „wzorzec programowy” pojawiająca się na rys. 4.89). Przykład pól PT dla pojedynczego cyklu pokazano na rysunku 4.90. Zawartość pola PT odczytywana jest przez wszystkie stacje. Zmiany w organizacji cyklu mogą być dokonane wyłącznie przez stację CM.

IMC (ang. *Isochronous Maintenance Channel*) - kanał ten przeznaczony jest dla ruchu izochronicznego. Obecnie nie jest zdefiniowany.



Rys. 4.89. Nagłówek pojedynczego cyklu



R - kanał WBC przeznaczony dla transmisji zwykłych pakietów  
S - kanał WBC będący kanałem izochronicznym

Rys. 4.90. Przykład pól PT pojedynczego cyklu

- **Szczeliny Dedykowane Transmisjom Asynchronousnym DPG** (ang. *Dedicated Packet Group*) - Pole to gwarantuje minimalną przepustowość dla transmisji normalnych ramek (ruch asynchronouszny lub synchroniczny) w standardzie FDDI. Przepustowość ta wynosi 0.708 Mb/s (12 bajtów cyklu).
- **Kanal szerokopasmowy WBC** (ang. *Wideband Channel*) - Pojedynczy kanał składa się z 96 bajtów w cyklu. WBC może być wykorzystany jako kanał izochroniczny (do komutacji połączeń) lub asynchronouszny (do komutacji pakietów). W sieci o przepustowości 100Mb/s możliwe jest utworzenie 16-u kanałów WBC o przepustowości po 6.144 Mb/s. Każdy kanał WBC, który przestaje być wykorzystywany do komutacji połączeń (obsługi ruchu izochronicznego), dołączany jest do kanału DPG i innych kanałów WBC nie będących kanałami izochronicznymi. Powstaje w ten sposób jeden kanał PDC (ang. *Packet Data Channel*) o dużej przepustowości, w którym dostęp do medium realizowany jest zgodnie ze standardem FDDI.

Rozdział przepustowości sieci pomiędzy różne typy kanałów ilustruje tabela 4.11. Kontrola kanałów WBC odbywa się na poziomie podwarstwy I-MAC. Każdy kanał WBC może być podzielony na podkanały umożliwiające jednoczesną, niezależną i izochroniczną wymianę danych pomiędzy parami stacji FDDI II. Unika się w ten sposób nadmiernego wzrostu liczby kanałów WBC przydzielonych do obsługi ruchu izochronicznego, i nieoptymalnego ich wykorzystania. Możliwy podział kanału WBC przedstawiono w tabeli 4.12.

Tabela 4.11. Rozdział przepustowości sieci pomiędzy różne typy kanałów

Bit/y cykl	Przepływność kb/s	Możliwe zastosowanie
1	8	Skompresowany głos, dane
2	16	Skompresowany głos, dane
4	32	Skompresowany głos, dane
8	64	Głos, kanał B w ISDN
48	384	6 kanałów B, kanał H0 ISDN
192	1536	24 kanały B, kanał H11 ISDN
192+1	1544	system T1
240	1920	30 kanałów B, kanał H12 ISDN
256	2048	system E1
768	6144	kanał WBC

Tabela 4.12. Podział przepływności kanału w sieci FDDI II

	Liczba bitów na cykl	Przepływność Mb/s
Preambuła + nagłówek	116	0.928
N kanałów izochronicznych (WBC)	N*768	N*6.144
Przepływność przeznaczona na transmisje pakietów (transmisje asynchroniczne i synchroniczne)	96+(16-N)*768	0.768+(16-N)*6.144
Razem	12500	100

### Inicjowanie pracy pierścienia

Zgodnie z algorytmem FDDI II pierścień rozpoczyna pracę w trybie podstawowym, uruchamiając proces żądania tokena w podwarstwie P-MAC. Przełączenia na tryb hybrydowy dokonuje stacja CM. **Przełączenie na tryb hybrydowy może być dokonane przez:**

- stację monitorującą, nabywającą prawa stacji CM bez procesu rywalizacji. Muszą przy tym być spełnione warunki:

1. w pierścieniu obecne są stacje mogące pracować w trybie innym niż podstawowy,
2. nie ma innych stacji CM,
3. stacja monitorująca przechwyciła token lub wygrała proces żądania tokena.

W chwili przejęcia tokena stacja nadaje cykl z następującymi ustawieniami: C1=R, C2=S, w CS odpowiedni numer cyklu, a pola PT uzupełniane są przez podwarstwę SMT.

W kolejnych stacjach przełączenie na tryb hybrydowy następuje po otrzymaniu pierwszego cyklu. Stacja inicjująca ten proces czeka, aby upewnić się, czy cykle poprawnie obiegają pierścień. Jeśli wszystko działa poprawnie stacja ta zostaje stacją CM; podwarstwy P-MAC i I-MAC połączone zostają zgodnie z zawartością pól PT. Nadawane są cykle z C1=S i C2=S.

- stację monitorującą, która wygrała proces rywalizacji. W procesie tym spośród wszystkich potencjalnych stacji monitorujących wybiera się tę, która posiada najwyższą pozycję w rankingu wszystkich stacji.

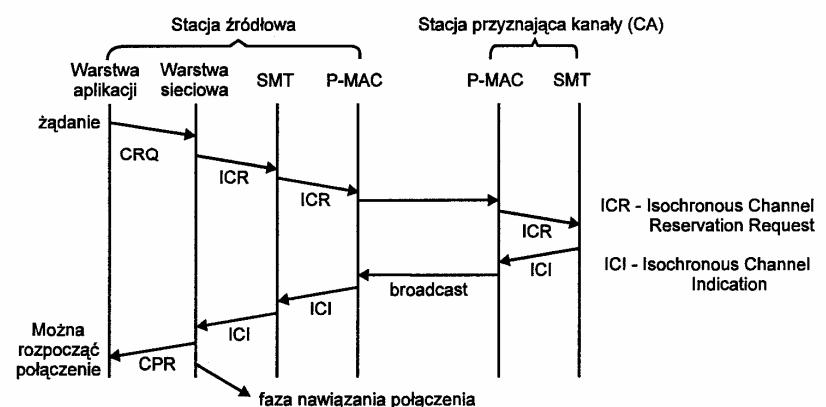
O pozycji stacji w rankingu decyduje kombinacja 8 bitów ustawianych przez administratora i 48 bitów adresu MAC. Podczas procesu rywalizacji wszystkie uczestniczące stacje generują cykle z C1=R i C2=R, a pole CS zawiera aktualną pozycję stacji w rankingu. Stacja na pierwszej pozycji zostaje stacją CM.

### Zmiana ustawień pola PT

Za zmianę ustawień pola PT odpowiedzialna jest stacja CM. W celu dokonania takiej zmiany stacja musi przechwycić token krążący w kanale PDC. Następnie zmieniane są poszczególne elementy pola PT i zainicjowany zostaje nowy cykl, a zaraz potem wysłany token. Pozostałe stacje modyfikują konfigurację kanałów WBC przy udziale funkcji podwarstwy SMT.

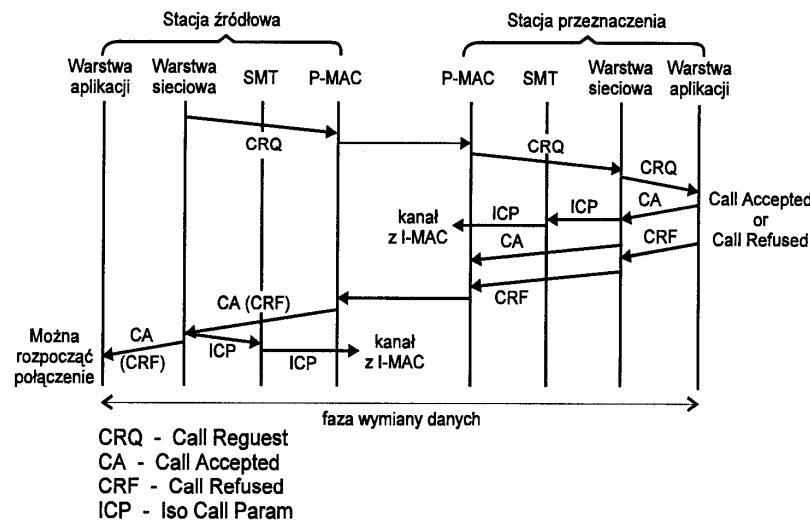
### Nawiązanie połączenia

Nawiązanie połączenia inicjowane jest przez aplikację stacji źródłowej. Wysyła ona żądanie nawiązania połączenia do warstw niższych modelu ISO. Warstwa sieciowa w tym modelu ustala adres MAC stacji przeznaczenia oraz określa, czy połączenie ma być nawiązywane lokalnie (np. inną aplikację w tej samej stacji) czy będzie to połączenie zdalne. W przypadku połączenia lokalnego nie ma potrzeby stosowania kanałów izochronicznych. Jeśli żądane jest połączenie z odległą stacją, wtedy do podwarstwy SMT wysłane zostaje żądanie rezerwacji kanału izochronicznego. Przykład rezerwacji kanału izochronicznego pokazano na rysunku 4.91.



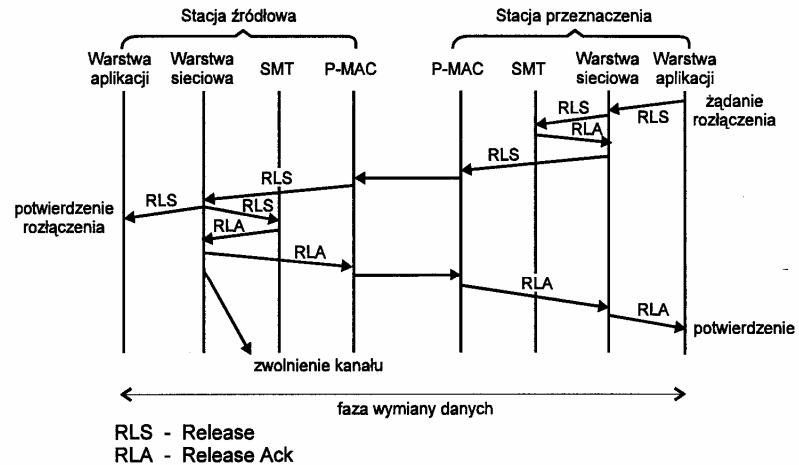
Rys. 4.91a. Rezerwacja kanału izochronicznego

W pierścieniu stacji wyodrębniona jest jedna stacja odpowiedzialna za przydział kanałów. Stacja ta nazywana jest dyspozycorem kanałów CA (ang. *Channel Allocator*). Podwarstwa SMT stacji wyrażającej chęć zainicjowania połączenia wysyła do CA żądanie przyznania kanału, korzystając przy tym z protokołu podwarstwy MAC. Jeśli w danej chwili istnieje kanał o pożądanej charakterystyce (o odpowiedniej przepustowości), podwarstwa SMT w stacji CA rezerwuje ten kanał wstawiając w nim adresy źródła i przeznaczenia informacji. Następnie wysyła tę informację do wszystkich obiektów SMT. Informacja o przyznaniu kanału dociera do warstwy sieciowej stacji-źródła. W tym samym czasie wysyłane są do stacji przeznaczenia dodatkowe, szczegółowe informacje odnośnie rozpoczęcia połączenia. Jeśli stacja docelowa zaakceptuje te warunki, wówczas jej warstwa sieciowa wysyła żądanie otwarcia kanału izochronicznego. Procesy podwarstwy I-MAC inicjują połączenie o żądanej charakterystyce. W tym momencie warstwa sieciowa informuje aplikację o nawiązaniu połączenia i możliwości transmisji danych w żadanym kanale (rysunek 4.91).

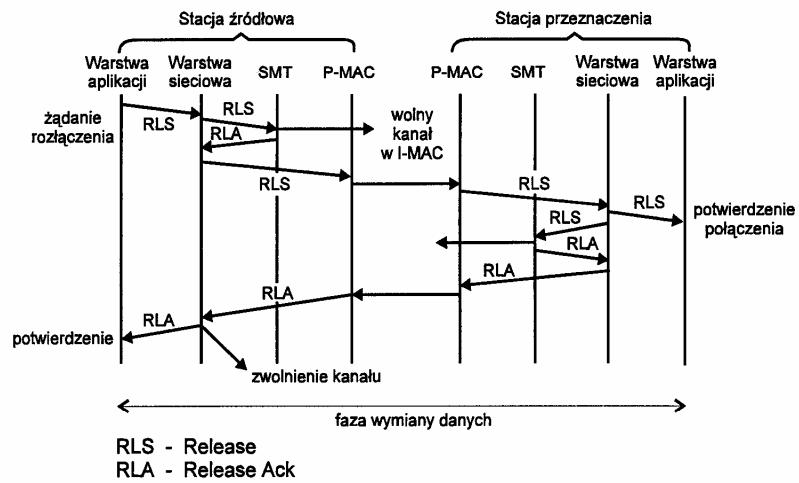


### Rozłączenie połączenia

Rozłączenie połączenia może zostać zainicjowane zarówno przez źródło jak i przez stację docelową. Podobnie jak nawiązywanie połączenia również rozłączenie odbywa się przy udziale podwarstwy SMT. Na rysunkach 4.92a i 4.92b zobrazowano sposoby realizacji rozłączenia zainicjowane przez stację przeznaczenia (rysunek 4.92a) lub przez stację źródłową (rysunek 4.92b).

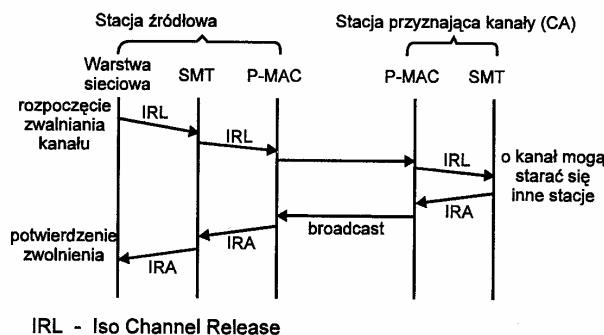


Rys. 4.92a. Rozłączenie połączenia rozpoczęte przez stację przeznaczenia



Rys. 4.92b. Rozłączenie połączenia rozpoczęte przez stację źródłową

W chwili wysłania lub otrzymania potwierdzenia o rozłączeniu RLA, warstwa sieciowa w stacji źródłowej wysyła informację o rozłączeniu do podwarstwy SMT w stacji CA. W CA odpowiednie procesy usuwają informację o zajętości kanału, rozsygając następnie wiadomość o zwolnieniu kanału do wszystkich SMT (patrz rysunek 4.92c).



Rys. 4.92c. Zwolnienie kanału

#### 4.2.9 Protokół DQDB z rozproszoną kolejką i podwójną magistralą - Standard IEEE 802.6

**Protokół DQDB** (ang. *Distributed Queue Dual Bus*), tj. *protokół z rozproszoną kolejką i podwójną magistralą*, jest akceptowany jako standardowy algorytm dostępu do medium (standard IEEE 802.6) w sieci metropolitalnej MAN. Jest on też traktowany jako jeden z potencjalnych elementów architektury logicznej dla sieci B-ISDN (ang. *Broadband-Integrated Services Digital Networks*).

##### 4.2.9.1 Uwagi ogólne i podstawowe parametry

Bardzo ważną cechą standardu IEEE 802.6 MAN jest to, że łączy on cechy zarówno sieci LAN jak też sieci B-ISDN ATM. Staje się tym samym użytecznym algorytmem pracy sieci metropolitalnych. Podstawowe cechy DQDB, które mogą być porównywane z cechami sieci LAN, bądź systemów ATM, są następujące:

- **Wspólne medium transmisyjne**

Standard IEEE 802.6 pozwala na dostęp do szerokopasmowego medium różnych klas stacji i obsługę różnych typów ruchu; zarówno synchronicznego, asynchronicznego jak też ruchu izochronicznego. Dostępne w DQDB przepustowości medium znacznie przekraczają przepustowości standardowych sieci LAN.

- **Wysoka szybkość transmisji**

IEEE 802.6 oferuje szeroki zestaw wspomaganych przez standard szybkości pracy. Podstawowy standard specyfikuje pracę z szybkością 44.7 Mb/s. Opracowywane opcje standardu dopuszczać będą transmisje z szybkościami od 1.544 Mb/s do 155 Mb/s. Szybkości te pokrywają zakresy pracy zarówno sieci IEEE 802 LAN jak i B-ISDN.

- **Dostosowanie IEEE 802.6 do współpracy z 802.2 LLC**

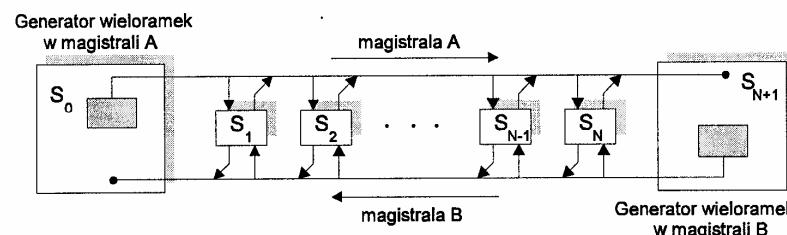
Standard przewiduje obsługę danych w warstwie WŁD w trybie bezpołączniowym (LLC-1) oraz połączeniowym. Dodatkowo IEEE 802.6 oferuje usługi izochroniczne.

- **Różnorodna adresacja**

Stacje DQDB muszą rozpoznawać adresy 48-bitowe oraz adresy 16-bitowe stosowane w sieciach LAN. Dodatkowo, opcjonalnie, stacje DQDB będą mogły stosować adresy 60-cio bitowe zalecane przez CCITT; tym samym zapewnione zostanie dopasowanie IEEE 802.6 do wymagań ISDN.

- **Stała długość ramki**

IEEE 802.6 narzuca stałą długość ramek wprowadzanych do medium równą 53 bajty (z 48-mioma bajtami danych). Zapewnia to dopasowanie do wymagań ATM, gdzie komórki mają identyczną długość (53 bajty). Jednakowa długość ramek gwarantuje wysoką efektywność obsługi wiadomości o różnych długościach, a w szczególności efektywny przekaz ruchu izochronicznego. Zwróćmy przy tym uwagę na fakt, że stała długość nie jest wymagana w żadnym innym standardzie IEEE 802.



Rys. 4.93. Struktura sieci MAN pracującej zgodnie z protokołem DQDB

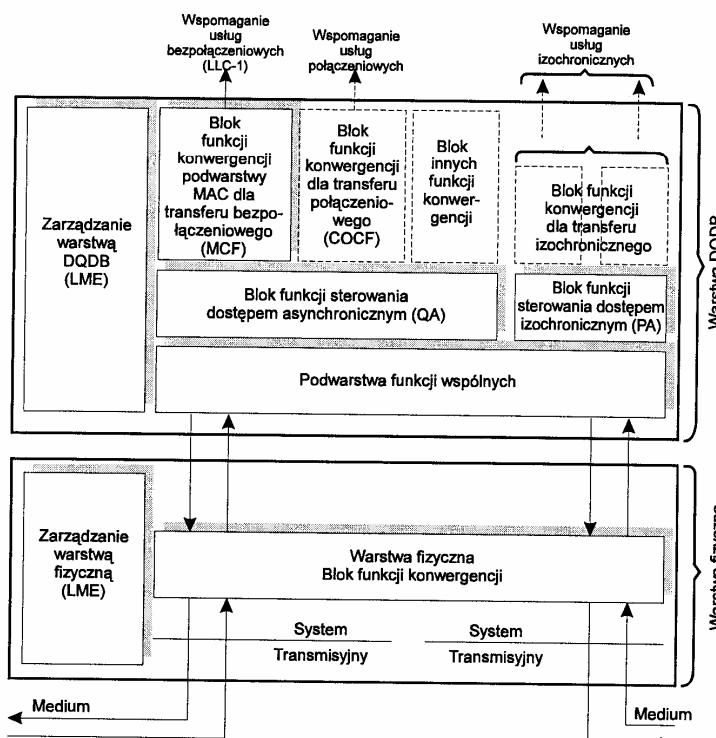
Algorytm DQDB, stanowiący poważną konkurencję dla FDDI, został zaprojektowany dla sieci z dwiema jednokierunkowymi magistralami, zgodnie z ilustracją pokazaną na rysunku 4.93. Sieć taka pozwala na realizację połączeń duplexowych między dowolną parą stacji (węzłów). Stacje dołączone są do magistrali za pomocą urządzeń stykowych pozwalających na odczytywanie danych z magistrali, jak też wprowadzenie do niej danych. Wprowadzanie danych do magistrali w trybie asynchronicznym odbywa się w wyniku realizacji procesu rezerwacji szczezin czasowych, z wykorzystaniem dwóch liczników odliczających liczbę szczezin zarezerwowanych przez pewną grupę stacji (licznik RQ-request) i liczbę szczezin bezpośrednio poprzedzających dostęp stacji do medium (licznik CD-countdown). Transmisje informacji w trybie izochronicznym poprzedzane są procesem uzgadniania warunków przekazu danych, a dostęp do specjalnie oznakowanych szczezin czasowych jest cykliczny. Transmisje w obu magistralach sieci DQDB są niezależne. Tym samym efektywna szybkość transmisji w sieci jest dwa razy wyższa od szybkości w magistrali.

#### 4.2.9.2 Architektura logiczna sieci DQDB

Podobnie jak we wcześniej omawianych standardach sieci LAN serii IEEE 802 również w standardzie IEEE 802.6 wyróżnia się trzy warstwy (ewentualnie podwarstwy) odpowiadające dwóm najniższym warstwom modelu ISO-OSI. Są to - poczynając od warstwy najwyższej:

1. Warstwa LLC-DQDB,
2. Warstwa DQDB (DQDB Layer),
3. Warstwa fizyczna.

Pierwsza z tych warstw, a mianowicie LLC-DQDB, odpowiada części warstwy WŁD w modelu OSI, bądź podwarstwie LLC w architekturze IEEE 802. Należy przy tym zwrócić uwagę na to, że w architekturze sieci DQDB podwarstwa LLC-DQDB stanowi zespół kilku różnych protokołów, których opis nie jest przedmiotem standardu IEEE 802.6. Usługi realizowane przez tę warstwę pozwalają jednakże na zdefiniowanie usług i funkcji jakie podsieć DQDB, a przede wszystkim warstwa DQDB, musi dostarczać.



Rys. 4.94. Organizacja wewnętrzna warstw DQDB

Organizacja wewnętrzna tych warstw pokazana jest na rysunku 4.94. Funkcje realizowane przez poszczególne warstwy oraz wzajemne relacje między warstwami są opisane poniżej.

#### Usługi DQDB

Standard IEEE 802.6 zakłada, że podwarstwa LLC-DQDB świadczy obiekтом warstw wyższych trzy typy usług. Są to:

1. Usługa bezpołączeniowa bez powiadomień (protokół LLC-1);
2. Usługa połączeniowa;
3. Usługa izochroniczna.

W przypadku usługi bezpołączeniowej typu LLC-1 dopuszcza się obsługę bloków informacji o długościach do 9188 bajtów. Bloki te są następnie, w warstwie DQDB dzielone na 52 bajtowe segmenty. Usługa bezpołączeniowa dostarczana przez warstwę DQDB (nazywana zwykle bezpołączeniową usługą MAC) obejmuje więc procedury segmentacji/resegmentacji wiadomości.

Usługa połączeniowa wspomagana przez DQDB pozwala na przekaz segmentów 52 bajtowych z wykorzystaniem kanałów wirtualnych. Również i usługa połączeniowa DQDB musi mieć wbudowane funkcje segmentacji i resegmentacji wiadomości. Należy przy tym podkreślić fakt, że funkcje sterowania i zarządzania połączonymi w kolejnych fazach zestawiania, utrzymywania i rozłączania nie są objęte standardem IEEE 802.6.

Ostatnia z oferowanych usług, tzw. usługa izochroniczna zapewnia użytkownikom dostęp do medium w cyklicznie powtarzających się okresach (identycznie jak w sieci FDDI II). Komunikacja między obiektami LLC odbywa się za pośrednictwem logicznego połączenia izochronicznego. Zasady sterowania tym połączeniem nie są objęte standardem IEEE 802.6.

#### Warstwa DQDB

Warstwa DQDB odpowiada w zasadzie podwarstwie MAC w sieciach LAN. Warstwa ta jest podzielona organizacyjnie na trzy podwarstwy:

- podwarstwę konwergencji-zgodności (ang. ConF - *Convergence Functions*),
- podwarstwę sterowania dostępem (ang. AF - *Arbitrated Functions*),
- podwarstwę funkcji wspólnych (ang. ComF - *Common Functions*).

Dodatkowo definiowany jest też blok (obiekt) zarządzania warstwą DQDB oraz styk do komunikacji z procesami zarządzania siecią.

Wymiana informacji pomiędzy obiektami LLC-DQDB i DQDB odbywa się z udziałem pomytywów operacyjnych typu żądanie i powiadomienie, odmiennych dla różnych usług dostarczanych przez warstwę DQDB.

W przypadku bezpołączeniowej usługi MAC (wspomaganie usługi LLC-1) używane są operacje podstawowe:

MA-UNIDATA.request

MA-UNIDATA.indication

MA-STATUS.indication.

Z kolei przy przekazie izochronicznym wymiana jednostek danych odbywa się z pomocą prymitywów

ISU-DATA.request

ISU-DATA.indication.

W zależności od rodzaju świadczonej usługi, w procesie nadawania/odbioru informacji zaangażowane są różne procedury będące elementami podwarstw: konwergencji (ConF), arbitracji dostępu (AF) i funkcji wspólnych (ComF) (zgodnie z zasadami architektury logicznej DQDB).

**Pierwsza podwarstwa warstwy DQDB tj. podwarstwa konwergencji** realizuje funkcje analogiczne do realizowanych przez podwarstwę adaptacji AAL w sieciach B-ISDN ATM. Funkcje te wiążą się z dostosowaniem wielkości ramek i ich zawartości do postaci wymaganej w sieci. W podwarstwie konwergencji specyfikowane są trzy rodzaje oferowanych usług. Są to:

1. bezpołączeniowy przekaz danych,
2. transmisje izochroniczne (usługa analogiczna do oferowanej w FDDI II),
3. połączeniowo - zorientowany przekaz informacji.

Za realizację usług bezpołączeniowych odpowiedzialny jest zespół funkcji konwergencji MCF (ang. *MAC Convergence Functions*) obejmujący procedury segmentacji i resegmentacji jednostek danych LLC-PDU (MAC SDU) przekazywanych z/do obiektu LLC.

W procesie transmisji poszczególne jednostki danych LLC-PDU, o długościach do 9188 bajtów, uzupełniane są w bloku MCF o nagłówki i zakończenie (proces enkapsulacji LLC-PDU), tworząc w ten sposób bloki IM PDU (ang. *Initial MAC PDU*). W następnej fazie obróbki w MCF ciągi IM PDU są dzielone na segmenty jednostkowe o długościach 44 bajtów każdy. W przypadku segmentów końcowych EOM (bądź wiadomości SSM jednosegmentowej) dokonywane jest ich uzupełnianie do pełnej długości 44 bajtów. W kolejnym kroku algorytmu tworzone są 48 bajtowe segmenty DM PDU (ang. *Derived MAC PDU*). Segmente te przekazywane są następnie do bloku QA podwarstwy dostępu AF - odpowiedzialnego za asynchroniczny przekaz segmentów jedną z magistrali sieci DQDB.

W procesie odbioru informacji blok MCF dokonuje resegmentacji wiadomości LLC-PDU.

Podstawowe fazy przetwarzania wiadomości przy nadawaniu i odbiorze bloków LLC-PDU ilustruje rysunek 4.95.

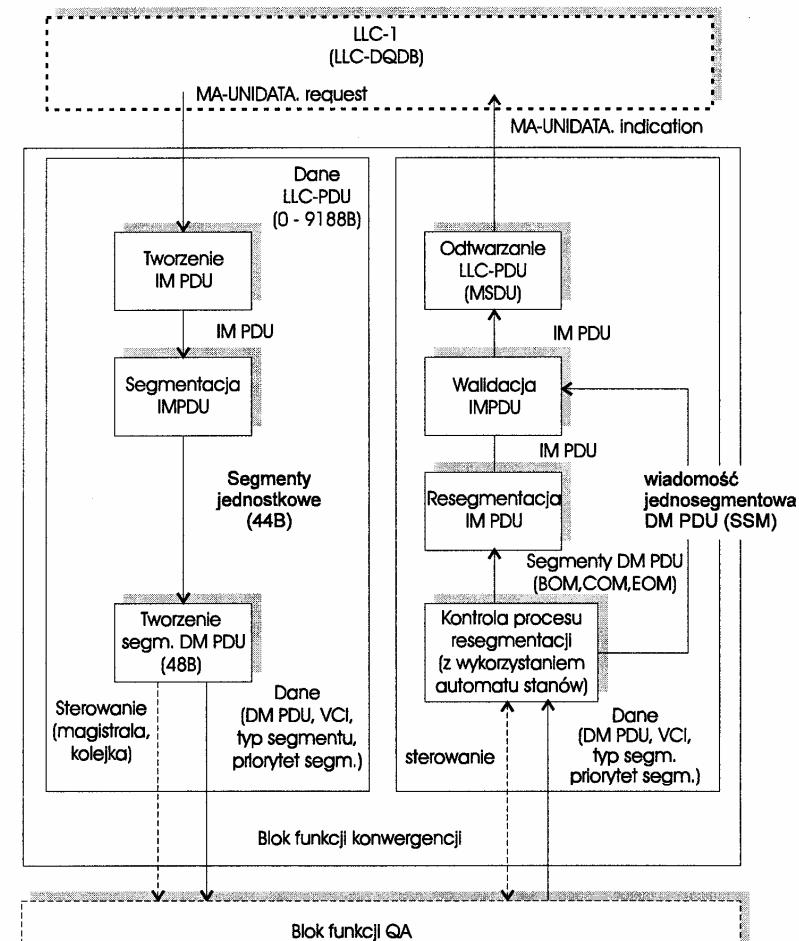
Do jednoznacznego odtworzenia ciągu segmentów po stronie odbiorczej służą między innymi:

- adresy MAC-owe stacji (pole DA, SA) zawarte w segmencie początkowym BOM - otrzymanym w wyniku podziału jednostki IM PDU

#### 4.2.9 Protokół DQDB z rozproszoną kolejką i podwójną magistralą - Standard IEEE 802.6

oraz

- identyfikatory wiadomości MID przydzielane każdej jednostce danych IM PDU przez blok funkcji wspólnych i zawarte w nagłówku każdego segmentu DM PDU (zarówno początkowego BOM jak i kolejnych - COM oraz EOM).



Rys. 4.95. Kolejne fazy przetwarzania wiadomości w podwarstwie konwergencji świadczącej bezpołączeniowe usługi MAC (B jest oznaczeniem bajtu; w standardzie używanie jest pojęcie oktetu)

W realizowanym przez warstwę konwergencji procesie resegmentacji jednostek IM PDU i odtwarzania LLC-PDU przeprowadzane są procedury rozpoznawania i walidacji poszczególnych pól i całych segmentów.

W odniesieniu do usług połączeniowych funkcje konwergencji COCF (ang. *Connection-Oriented Convergence Functions*) nie zostały dotychczas zdefiniowane. Przyjmuje się jednakże, że COCF realizować będzie zespół tych samych, co w przypadku MCF, procedur segmentacji i resegmentacji wiadomości oraz wykorzystanie identycznych zasad współpracy (nadawanie/odbiór segmentów) z blokiem arbitracji dostępu QA do magistrali sieci DQDB.

Z kolei zespół izochronicznych funkcji konwergencji ICF (ang. *Isochronous Convergence Functions*) ma na celu dostosowanie izochronicznego przekazu danych do rytmu pracy mechanizmu gwarantowanego dostępu PA do medium. Jedną z podstawowych funkcji bloku ICF stanowi więc w tym przypadku buforowanie strumienia danych w celu ich dopasowania do rytmu napływu magistralą A lub B zarezerwowanych szczezin czasowych.

**Funkcje realizowane przez podwarstwę arbitracji dostępu AF** (ang. *Arbitrated Functions*) dotyczą przede wszystkim procedur odpowiedzialnych za sterowanie dostępu do medium; w szczególności dotyczą one dwóch typów dostępu: gwarantowanego i niegwarantowanego. Pierwszy typ wiąże się z realizacją usług izochronicznych i zapewnieniem dostępu do wcześniej przydzielonych danemu połączeniu szczezin czasowych (ang. PA - *PreArbitrated slots*). Funkcje związane z realizacją procedury PA obejmują uprzednie zestawienie połączenia izochronicznego i nadanie temu połączeniu identyfikatora VCI (ang. *Virtual Channel Identifier*). W przypadku dostępu niegwarantowanego (ang. *Queued Arbitrated - QA*) mamy do czynienia z rezerwacją szczezin QA. Szczeliny QA przenoszą ruch asynchroniczny. Szczegółowy opis procedur związanych z obsługą ruchu asynchronicznego zostanie podany w dalszej części tego rozdziału. W tym miejscu zamieścimy jedynie schematyczną ilustrację operacji realizowanych przez blok funkcji QA (patrz rysunek 4.96), odpowiedzialny za asynchroniczny przekaz informacji i wspomagający bezpołączeniowe i połączeniowe usługi DQDB.

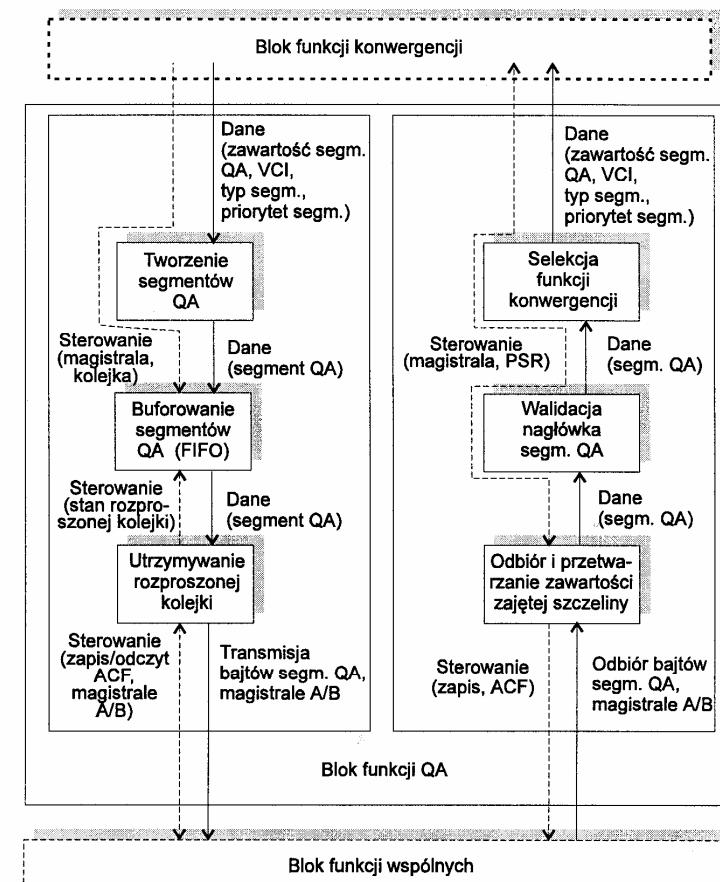
Segmenty QA tworzone w bloku QA stanowią powiększone o pole nagłówka segmenty DM PDU odbierane z bloku funkcji konwergencji. Znajdujące się w nagłówku segmentu QA (bądź PA) 20-bitowe pole VCI stanowi identyfikator połączenia wirtualnego. W przypadku usługi bezpołączeniowej wszystkie bity VCI są jedynkami. Pole VCI pozwala jednakże w sposób jednoznaczny identyfikować połączenie logiczne w przypadku realizacji usługi połączeniowej bądź usługi izochronicznej.

**Procedury realizowane przez podwarstwę funkcji wspólnych ComF** wiążą się z:

- desygnowaniem dwóch stacji końcowych (ang. *Head-of-Bus Function*) jako stacji zarządzających siecią oraz generacją i transmisją przez te stacje szczezin (ramek) czasowych zawierających znaczniki szczezin

(określające przeznaczenie poszczególnych szczezin - asynchroniczne/izochroniczne) oraz identyfikatory kanałów wirtualnych;

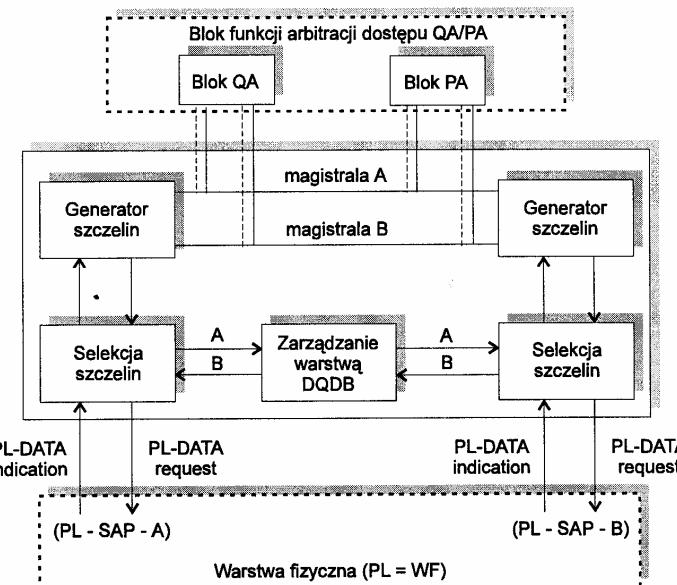
- inicjowaniem pracy sieci i jej rekonfiguracją, w przypadku uszkodzenia (ang. *Configuration Control Function*);
- przydzielaniem wiadomości specjalnych identyfikatorów MID, niezbędnych w procesie ich segmentacji/resegmentacji (ang. *Message - ID Page - Allocation Function*). Procedury MID są realizowane w sieci w sposób rozproszony, gwarantując jednoznaczność interpretacji wartości ID.



Rys. 4.96. Schematyczna ilustracja operacji realizowanych przez Blok Funkcji QA przy nadawaniu i odbiorze segmentów QA

Po przydiale jednostce danych IM PDU identyfikatora MID, identyfikator ten jest wprowadzany do każdego segmentu DM PDU tworzącego IM PDU. Zapewnia to logiczny związek pomiędzy segmentami tej samej jednostki danych. Elementem tej podwarstwy jest też blok zarządzania warstwą DQDB. Wybranym zagadnieniom zarządzania pracą warstwy DQDB i całej sieci poświęcimy nieco uwagi w jednym z kolejnych paragrafów książki. Należy jednakże zwrócić uwagę na fakt, że po odbiorze przez stację docelową pierwszego elementu BOM wiadomości LLC-PDU w stacji tej uruchamiany jest zegar. Jeżeli ostatni segment EOM napłynie po upływie czasu time-out-u, wówczas wszystkie segmenty danej IM PDU zostają odrzucone.

Organizację pracy podwarstwy funkcji wspólnych ilustruje rysunek 4.97.

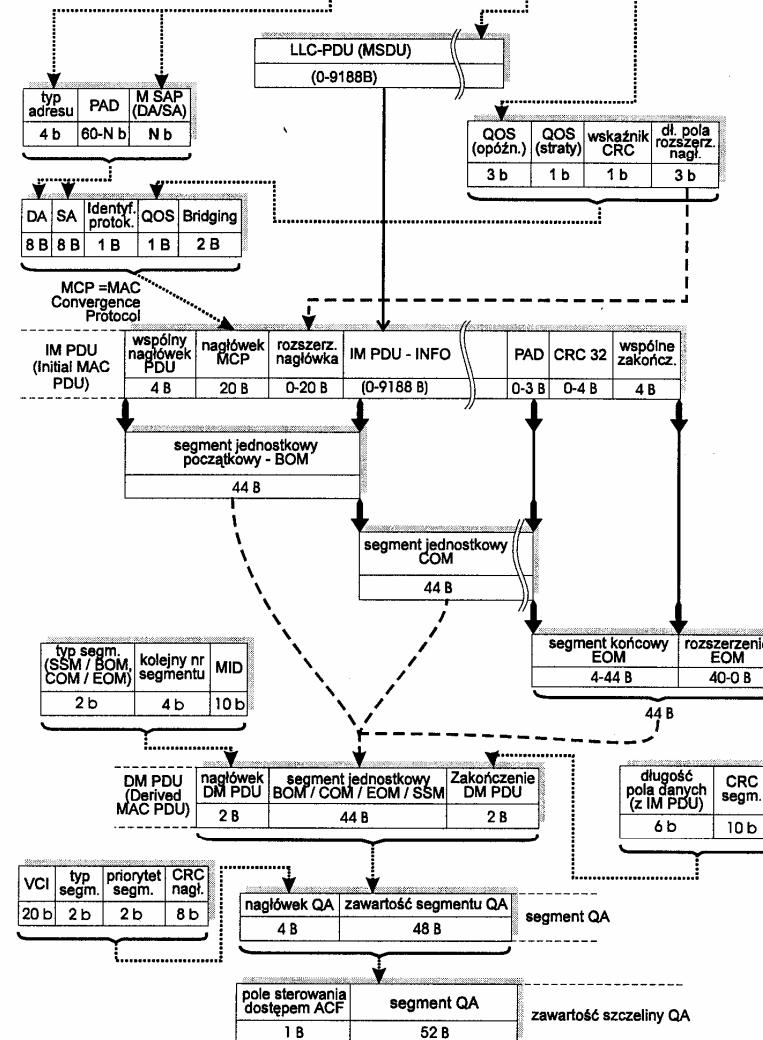


Rys. 4.97. Ilustracja procedur realizowanych przez podwarstwę funkcji wspólnych

Z załączonego powyżej opisu funkcji warstwy DQDB wynika, że w procesie przekazu jednostek LLC-PDU pomiędzy obiektami LLC w komunikujących się stacjach ma miejsce szereg przekształceń tych jednostek, związanych między innymi z enkapsulacją LLC-PDU, segmentacją IM PDU, dodawaniem nagłówków i zakończeniem do jednostek danych. Ciąg powyższych przekształceń w odniesieniu do wymiany bezpołączeniowej (bądź też zorientowanej połączeniowo) ilustruje rysunek 4.98. Na rysunku tym podano też znaczenia wybranych pól podlegających przekształcaniu jednostek danych. Otrzymywane w wyniku tych

przekształceń segmenty QA są następnie przekazywane do warstwy fizycznej i transportowane, jedną z dwóch magistral, do stacji docelowej.

MA - UNIDATA request (SA - adres źródłowy, DA - adres docelowy, dane, priorytet, klasa usługi)

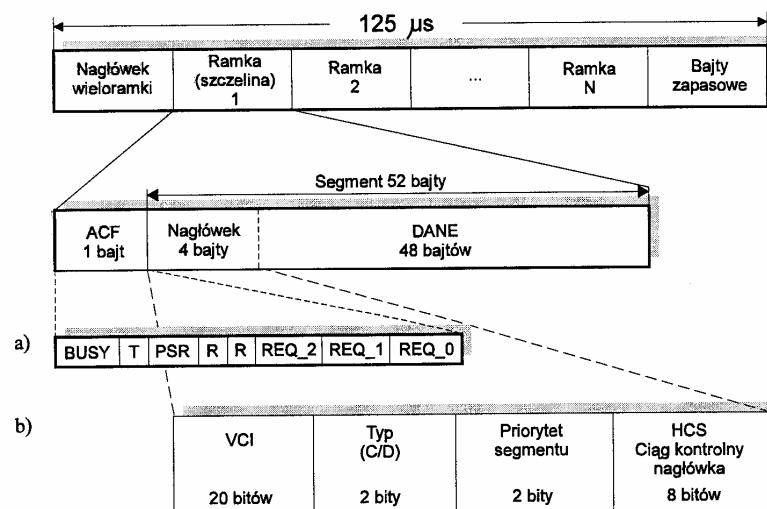


Rys. 4.98. Przekształcenia informacji w przypadku bezpołączeniowego transferu danych (LLC-1 - bezpołączeniowa usługa MAC); długości pól wyrażone są w bitach (b) lub bajtach (B)

W przypadku warstwy fizycznej standard IEEE 802.6 definiuje trzy podstawowe opcje pozwalające na współpracę z następującymi systemami transmisyjnymi:

- ANSI DS3 - dla transmisji z szybkościami 44.736 Mb/s z wykorzystaniem kabli koncentrycznych i światłowodów;
- ANSI SONET (lub CCITT SDH) - dla szybkości transmisji 155.52 Mb/s (i większych) z wykorzystaniem światłowodów jednomodowych;
- CCITT G.703 - dla szybkości transmisji 34.368 Mb/s z wykorzystaniem mediów przewodowych (przewody miedziane).

#### 4.2.9.3 Format ramki/szczeliny czasowej i struktura ramki QA



Rys. 4.99. (a) Struktura ramki w DQDB (b) Struktura nagłówka ramki DQDB

Przekaz informacji w poszczególnych magistralach odbywa się za pośrednictwem szczelin/komórek o długości 53 bajtów, których ogólna struktura została pokazana na rysunku 4.99. Poszczególne stacje odczytują i kopią dane zawarte w szczelinach czasowych przepływających przez urządzenia stykowe. Mogą one również uzyskiwać dostęp do sieci wprowadzając swoje informacje do szczelin. Stacje skrajne sieci: stacja początkowa  $S_0$  magistrali A i stacja  $S_{N+1}$  początkowa magistrali B generują ciągi sygnałów synchronizacji w obu magistralach. Ciągi te wyznaczają początki wieloramki o długościach 125 μs. Przykładowa struktura wieloramki w magistrali A pokazana jest na rysunku 4.99. Każda wieloramka podzielona jest pewną liczbą szczelin (ramek czasowych). Stacja końcowa, dla danej magistrali, usuwa wszystkie napływające do niej ramki; i tak

stacja  $S_{N+1}$  usuwa wieloramki z magistrali A i generuje (niekoniecznie w tych samych chwilach) ramki czasowe w magistrali B. Podobną funkcję w magistrali A pełni stacja  $S_0$ , która jest zwykle stacją główną w sieci DQDB.

Pojedyncza ramka czasowa o strukturze pokazanej na rysunku 4.99 posiada następujące pola/znaki:

- pole sterujące** (ang. ACF - Access Control Field) obejmujące osiem bitów o poniższym znaczeniu:

B - bit zajętości ramki czasowej (B=0-ramka wolna);

T - bit typu szczeliny/usługi (T=0-usługa asynchroniczna, T=1-usługa izochroniczna);

PSR - 1 bitowe pole (previous slot received) wskazujące, czy poprzednia szczelina została wykorzystana (PSR=1) czy też nie (PSR=0). Bit PSR ustawia ta stację, do której adresowana jest zawartość szczeliny. PSR stwarza możliwość ponownego wykorzystania zwolnionej szczeliny;

R - 2 bity zarezerwowane do wykorzystania w przyszłości (np. do określenia priorytetu ramki), ustawiane jako 00;

REQ - 3 bitowe pole rezerwacyjne (ang. REQuests), umożliwia realizację rezerwacji szczelin.

- nagłówek ramki** obejmujący 4 bajty (32 bity):

VCI - identyfikator kanału wirtualnego. Kombinacja samych "0" oznacza brak przyporządkowania jakiejkolwiek stacji końcowej. Z kolei ciąg samych "1" oznacza przyporządkowanie typu QA (realizacja usługi bezpołączeniowej);

Typ (C/D) - 2 bity wskazujące na typ ramki (Control/Data);

Priorytet segmentu - do ewentualnego wykorzystania w przyszłości;

HCS - 8 bitów kontrolnych kodu cyklicznego generowanego przez wielomian  $G(x)=x^8+x^2+x+1$ , do zabezpieczenia nagłówka. Ciąg ten generowany jest przez węzeł początkowy dla szczelin typu PA, bądź przez węzeł zajmujący szczelinę w przypadku szczelin QA;

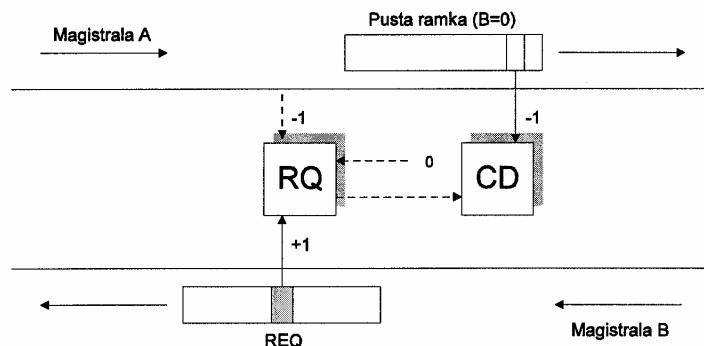
- dane użytkownika** (do 48 bajtów - jest to segment DM PDU).

W procesie rezerwacji szczelin i transmisji ramek informacyjnych następuje modyfikacja pola ACF i/lub uzupełnianie nagłówka i pola danych szczeliny czasowej. W przypadku transmisji izochronicznej, umieszczenie jednego bajtu w szczelinie PA jest równoważne utworzeniu kanału cyfrowego o przepustowości 64 kb/s. Umieszczając więcej bajtów w szczelinie (polu danych) otrzymujemy kanał o większej przepustowości.

#### 4.2.9.4 Zasada dostępu asynchronicznego (QA) do magistrali

W przypadku transmisji asynchronicznej ramki czasowe (szczeliny) przydzielały są stacjom na żądanie. Umieszczane są w nich fragmenty bądź segmenty

pakietów (wiadomości) gotowych do przekazu. **Sterowanie dostępem do magistrali odbywa się za pośrednictwem pola sterującego ramki czasowej ACF.** Przy transmisji bezpriorytetowej wykorzystywane są bity zajętości B oraz żądania obsługi REQ. Ustawienie bitu B=1 sygnalizuje, że dana szczelina czasowa jest już zajęta, a zatem niedostępna dla innego użytkownika. Bit REQ jest wykorzystywany przez stację do celów rezerwacji, tj. do poinformowania innych stacji o posiadaniu ramki (segmentu) gotowej do transmisji.



Rys. 4.100. Ilustracja pracy liczników RQ i CD, gdy stacja ma ramkę (segment) do nadania

Rozważmy pracę stacji, gdy segment ma być przesłany magistralą A. W takim przypadku bit REQ musi być przesłany magistralą B, tj. w kierunku przeciwnym do kierunku transmisji segmentu. W celu właściwego sterowania dostępem do medium wszystkie stacje ( $S_1, \dots, S_N$ ) utrzymują dwie pary (po jednej parze dla każdej magistrali) modyfikowanych dynamicznie liczników RQ i CD (patrz rysunek 4.100). Liczniki RQ służą do zliczania żądań obsługi REQ napływających np. magistralą B, a więc pochodzących od stacji o numerach wyższych od numeru  $S_i$  danej stacji. Każda pusta szczelina czasowa przepływająca poprzez układ stykowy stacji magistralną A powoduje zmniejszenie o 1 wartości stanu licznika RQ (w danej stacji). Jak łatwo zauważyci stan licznika RQ w danej stacji, zliczającego rezerwacje napływające magistralą B, odzwierciedla dokładnie stan rozproszonej kolejki ramek (segmentów) oczekujących na transmisję magistralą A w stacjach o numerach wyższych. (Analogicznie wygląda sytuacja w magistrali B). Kolejka ta jest obsługiwana w zasadzie zgodnie z regułą FIFO. W przypadku, gdy stacja ma do nadania segment QA, wówczas po nadaniu bitu REQ uruchamia drugi licznik CD, do którego przepisuje zawartość licznika RQ. Licznik RQ jest wówczas zerowany. Ilustruje to rysunek 4.100. Stan licznika CD jest więc początkowo równy liczbie szczelin czasowych zarezerwowanych przez stacje o numerach wyższych. Po każdorazowym pojawienniu się w interfejsie stacji wolnej szczeliny, stan licznika CD jest zmniejszany o 1. Gdy stan licznika

CD osiągnie wartość zero, stacja uzyskuje prawo dostępu do medium, tj. możliwość zajęcia kolejnej wolnej szczeliny. W trakcie oczekiwania na wyzerowanie się licznika CD stan licznika RQ może również ulegać zmianie, zgodnie z pojawianiem się lub brakiem nowych rezerwacji REQ.

Zauważmy przy tym, że wiadomości składające się z jednego segmentu są obsługiwane w kolejności napływu, natomiast wiadomości wielosegmentowe obsługiwane są w zasadzie cyklicznie, tj. zgodnie z zasadą round-robin. Z opisu protokołu DQDB wynika, że stacje położone bliżej czoła magistrali B (o wysokich numerach) są uprzywilejowane w dostępie do pustych szczelin w magistrali A. Ten sam wniosek odnosi się do węzłów skrajnych magistrali A.

Podsumowując powyższe rozważania możemy stwierdzić, że każda stacja może znaleźć się w jednym z trzech stanów:

- monitorowania - stacja nie posiada pakietu do wysłania, a jedynie analizuje wartości bitów REQ i B (ang. BUSY) oraz aktualnia wartości liczników RQ;
- oczekiwania - przejście stacji do tego stanu następuje po pojawienniu się w węźle ramki do transmisji. Stacja oczekuje na możliwość wysłania rezerwacji, aktualnia jednocześnie stan własnego licznika RQ. Dokonując rezerwacji stacja podejmuje stosowne działania, tzn. kopiuje zawartość licznika RQ do licznika CD, zeruje licznik RQ i ustawia bit REQ w polu ACF ramki w kanale;
- odliczania - do stanu tego stacja przechodzi po wysłaniu rezerwacji. Zmieniane są wtedy na bieżąco wartości liczników CD i RQ. RQ zlicza kolejne rezerwacje, gdy pojawia się szczelina z bitem REQ=1. Licznik CD zmniejsza stan, gdy magistralą przepływa szczelina z bitem B=0. W chwili, gdy CD osiągnie wartość 0, stacja umieszcza swój segment w najbliższej wolnej szczeliniie i przechodzi do stanu monitorowania.

**Zdecentralizowany algorytm rezerwacji dostępu DQDB zapewnia możliwość stosowania priorytetów.** Pozwala to na regulowanie dostępu do medium. Segmente z wyższymi priorytetami otrzymują wówczas szybszy dostęp do szczelin typu QA. **Zastosowanie priorytetów narzuca jednakże konieczność wyposażenia stacji w kolejne pary liczników RQ i CD.** Przy trzech różnych priorytetach obsługi każdy węzeł musi utrzymywać 6 liczników RQ, po jednym dla każdego priorytetu i każdej magistrali, oraz 6 liczników CD.

#### 4.2.9.5 Zasada dostępu izochronicznego (PA) do magistrali

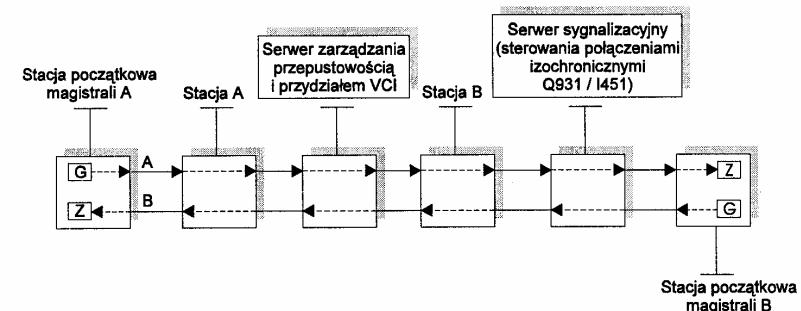
Algorytm dostępu do szczelin PA wspomaga izochroniczny przekaz danych pomiędzy obiektami LLC-DQDB. Szczeliny PA są, w tym trybie obsługi zgłoszeń, odpowiednio znakowane poprzez ustawienie wartości bitów zajętości i typu szczeliny (ang. slot type) w polu ACF. Kombinacja bitów: B=1, typ szczeliny=1 oznacza szczelinę PA. Znakowania szczelin dokonuje stacja początkowa magistrali, jako wynik procesu rezerwacji przez stację (np. z wykorzystaniem

serwerów: sygnalizacyjnego i przydzielu przepustowości oraz identyfikatorów VCI określonych zasobów sieciowych. Jedną z podstawowych funkcji węzłów początkowych jest też wpisywanie identyfikatorów kanałów wirtualnych do pola VCI szczelin PA. Dostęp do szczeliny jest możliwy po sprawdzeniu przez stację zgodności identyfikatora VCI szczeliny PA, z wartością VCI przydzieloną stacji. Dla każdej przydzielonej wartości VCI stacja otrzymuje też informację o pozycjach bajtów, które w danej szczeliniie może zająć. W jednej szczelinie mogą więc być transportowane informacje (bajty) pochodzące z kilku stacji.

#### 4.2.9.6 Zarządzanie siecią DQDB

Standard DQDB specyfikuje szereg funkcji zarządzania pracą sieci DQDB, zarówno w odniesieniu do warstwy DQDB, jak też i warstwy fizycznej. Za zarządzanie lokalnymi funkcjami warstwy DQDB odpowiedzialny jest blok (obiekt) LME zarządzania warstwą DQDB (ang. *DQDB LME-DQDB Layer Management Entity*). Zapewnia on również komunikację z blokami (obiektami) LME w innych węzłach i prowadzi rozproszone zarządzanie zasobami warstwy DQDB. Funkcjonalnie DQDB-LME stanowi jeden z elementów warstwy funkcji wspólnych. Do celów wymiany informacji zarządzających służy protokół LMP zarządzania warstwą DQDB (ang. *DQDB LMP - DQDB Layer Management Protocol*) wspomagany w tym zakresie przez blok funkcji wspólnych DQDB. Standard IEEE 802.6 definiuje też interfejs DQDB LMI (ang. *DQDB Layer Management Interface*) specyfikujący prymitywy operacyjne pozwalające na sterowanie przekazem informacji zarządzających pomiędzy blokiem LME a blokiem NMP zarządzania siecią (ang. *Network Management Process*). Wymiana stosownych prymitywów pozwala na realizację sterowania procesami zestawiania połączeń, ich utrzymywania i rozłączania. W przypadku ruchu izochronicznego w standardzie IEEE 802.6 rozwija się możliwość wykorzystania, w procesie zestawiania i rozłączania połączenia między aplikacjami stacji A i B, ISDN-owskiego systemu sygnalizacji (zalecenie Q 931 - w odniesieniu do warstwy sieciowej), zaimplementowanego w serwerze sygnalizacyjnym, współpracującym z jednym z węzłów sieci. Poszczególne elementy funkcjonalne sieci DQDB zaangażowane w procesie zestawiania połączenia izochronicznego ilustruje rysunek 4.101. Żądanie połączenia izochronicznego jest każdorazowo kierowane do serwera sygnalizacyjnego, który z kolei inicjuje zespół działań mających na celu:

- rezerwację, w serwerze zarządzania przydzielem przepustowości i identyfikatorów VCI, odpowiednich zasobów sieciowych,
  - przydział połączeniu izochronicznemu identyfikatora VCI kanału wirtualnego
- oraz
- oznakowanie przez stację początkową magistrali szczelin PA przeznaczonych dla danego połączenia.



Rys. 4.101. Elementy funkcjonalne sieci DQDB biorące udział w procesie zestawiania połączenia izochronicznego (G - generator szczelin, Z - zakończenie magistrali)

Definiowany przez standard DQDB interfejs DQDB LMI specyfikuje następujące prymitywy i operacje podstawowe:

- LM\_SET\_VALUE.invoke
- LM\_SET\_VALUE.replay
- LM\_COMPARE\_AND\_SET.invoke
- LM\_COMPARE\_AND\_SET.replay
- LM\_GET\_VALUE.invoke
- LM\_GET\_VALUE.replay
- LM\_ACTION.invoke
- LM\_ACTION.replay
- LM\_EVENT.notify

Trzy definiowane powyżej prymitywy tj. invoke, replay i notify mają następujące znaczenia:

- *invoke* - są to prymitywy generowane przez procesy bloku NMP zarządzania pracą sieci (ang. *NMP - Network Management Process*), zlokalizowanego w danym węźle i kierowane do bloku LME z żądaniem dostarczenia stosownej usługi, tj. wymuszające na bloku LME realizację właściwych operacji zarządzania;
- *replay* - prymityw przesyłany z LME do NMP jako reakcja na prymityw invoke; replay przenosi informację o wynikach wcześniejszych działań;
- *notify* - prymityw przekazywany z bloku (obiektu) LME do bloku (obiektu) NMP z informacją o wystąpieniu w warstwie DQDB pewnych istotnych zdarzeń.

Z kolei operacje związane z powyższymi prymitywami mają następującą interpretację:

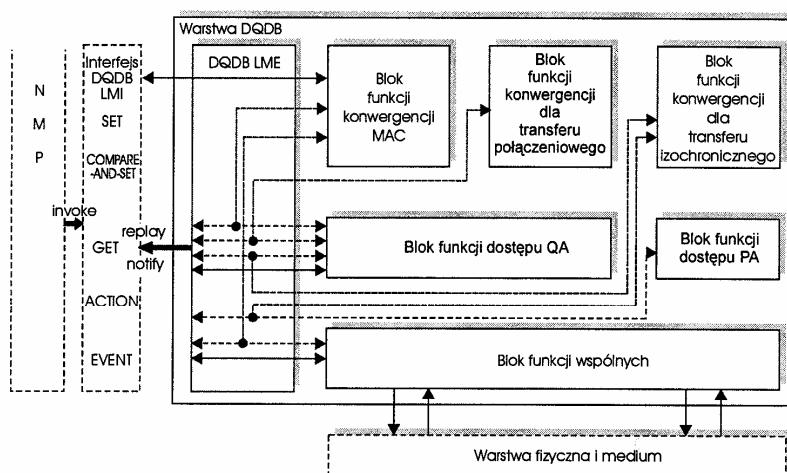
- SET - ustalenie pożąданiej wartości parametru,

- COMPARE-AND-SET - ustalenie pożąданej wartości parametru z równoczesnym przeprowadzeniem stosownego testu,
- GET - pobranie wartości określonego parametru,
- ACTION - działanie wymuszające zmianę pewnych stanów warstwy DQDB (przyjęcie określonego stanu lub zainicjowanie ciągu zdarzeń),
- EVENT - operacja inicjowana lokalnie przez blok LME w celu przekazania NMP informacji o istotnym zdarzeniu w warstwie DQDB.

Powyższe prymitywy reprezentują wzajemne interakcje Procesu Zarządzania Siecią (NMP) i bloku zarządzania DQDB LME. Oddziaływanie NMP dotycza w szczególności:

- zarządzania typami połączeń,
- przydziału identyfikatorów VCI,
- rozdziału identyfikatorów MID,
- przydziału adresów MAC-owych stacjom, w przypadku, gdy dana implementacja DQDB stosuje adresy inne niż 48-bitowe,
- zarządzania parametrami systemu DQDB,
- wyznaczania stacji końcowych magistrali,
- uzgadniania postaci nagłówków IM PDU (z rozszerzeniem lub bez).

Wzajemne relacje między blokiem zarządzania siecią NMP, blokami zarządzania DQDB LME i blokami funkcjonalnymi warstwy DQDB pokazuje rysunek 4.102.



Rys. 4.102. Wzajemne oddziaływanie pomiędzy NMP (Network Management Process), blokiem zarządzania LME DQDB i pozostałymi blokami funkcjonalnymi warstwy DQDB. Liniami przerywanymi zaznaczono jednocześnie oddziaływanie pomiędzy LME DQDB i dwoma innymi blokami DQDB

Przekazywanie informacji sterujących pomiędzy poszczególnymi obiekty LME DQDB odbywa się z wykorzystaniem protokołu zarządzania DQDB LME (ang. *DQDB Layer Management Protocol*). Zgodnie z tym protokołem informacje zarządzające przesyłane są za pomocą specjalnych bajtów typu DQDB Management. Częstotliwość generacji, przez stacje końcowe magistrali, pustych bajtów do celów zarządzania konfiguracją sieci i dystrybucji identyfikatorów MID, uzależniona jest przy tym od procedur konwergencji warstwy fizycznej (ang. *Physical Layer Convergence Procedure*) - i dostosowana do wymagań podsieci DQDB

#### 4.2.9.7 Jakość pracy sieci z asynchronicznym protokołem DQDB

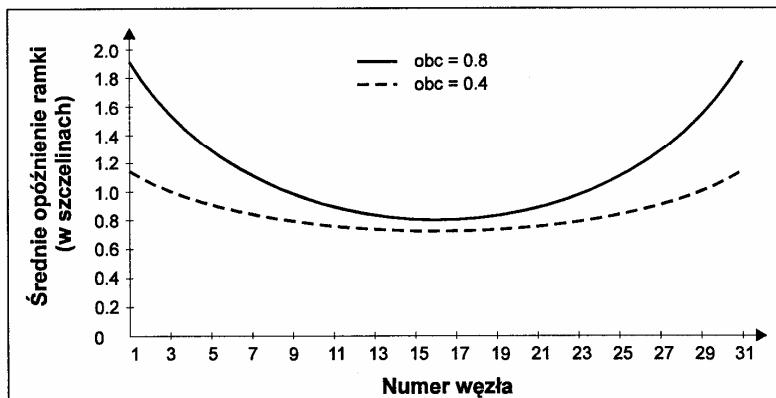
*Pracę protokołu DQDB cechuje wysoka wydajność wykorzystania medium. Wiąże się to z prostym i absorbującym nieznaczną część przepustowości sieci zdecentralizowanym algorytmem rezerwacji szczezin czasowych. Jednocześnie w pracy stacji obserwujemy zjawisko dyskryminowania bądź uprzewilejowywania w prawie dostępu do medium niektórych stacji sieci. Algorytm DQDB nie jest więc sprawiedliwy.* Aby ukazać ten fakt zaprezentujemy przykładowe wyniki analizy pracy sieci. Przedmiotem naszego zainteresowania będą średnie opóźnienia ramek w dostępie do kanału. Prezentowane wyniki uzyskano przy założeniu, że:

- czasy propagacji w kanale są pomijalnie małe w porównaniu z czasem transmisji ramki (jest to założenie nie zawsze spełnione w szybkich sieciach LAN lub MAN);
- każda stacja  $S_i$ ,  $i=1, \dots, N$  wyposażona jest w dwa bufore: lokalny i wyjściowy. Nowy pakiet generowany w stacji jest wprowadzany na koniec bufora lokalnego, w którym pozostaje do chwili, gdy zostanie dla niego wysłane żądanie rezerwacji szczezliny (REQ). Wówczas pakiet jest przesyłany do bufora wyjściowego, w którym oczekuje na transmisję;
- kolejna rezerwacja szczezliny przez daną stację może mieć miejsce dopiero po wysłaniu przez stację pakietu z bufora wyjściowego (bufor wyjściowy jest jednopakietowy). Zwróćmy uwagę na to, że czas przebywania ramki informacyjnej w buforze lokalnym zależy od zasad rządzących wysyłaniem rezerwacji przez stacje, natomiast czas przebywania w buforze wyjściowym uzależniony jest od stanu rozproszonej kolejki, czyli liczby wysłanych wcześniej rezerwacji;
- tylko jeden bit z pola REQ jest wykorzystywany przez stacje do celów rezerwacji;
- każda ze stacji generuje w czasie jednostkowym (jedna szczezliny) tylko jeden pakiet do wysłania z jednakowym prawdopodobieństwem  $P = 2\rho / (N + 1)$ ; gdzie  $\rho$  jest obciążeniem sieci tj. prawdopodobieństwem wygenerowania ramki kierowanej do jednej magistrali przez wszystkie stacje sieci w czasie jednej szczezliny.

Prawdopodobieństwo przesłania ramki, wygenerowanej przez wybraną stację, określona magistralą zależy oczywiście od położenia stacji w sieci. W przypadku stacji o numerze  $k$  prawdopodobieństwo przesłania ramki magistralą A wynosi  $P_{kA} = (N-k)/(N-1)$ , a magistralą B - odpowiednio  $P_{kB} = (k-1)/(N-1)$ . Na rysunku 4.103 przedstawiono zmiany opóźnień ramek otrzymane dla obciążen sieci  $\rho=0.4$  i  $\rho=0.6$  przy liczbie stacji  $N=31$ .

Krzywe otrzymane dla modelu z wiadomościami jednosegmentowymi i możliwością rezerwacji przez stacje tylko jednej szczeliny QA wskazują na wyraźne uprzywilejowanie w dostępie do medium stacji środkowych sieci DQDB (bez względu na wartość obciążenia  $\rho$ ).

Jeżeli odstępmy od powyższych założeń, zakładając przesyłanie wiadomości wielosegmentowych oraz możliwość jednorazowej rezerwacji przez stacje/stację większej od 1 liczby szczelin QA, to otrzymane wyniki mogą mieć charakter istotnie różny od ilustrowanego przebiegiem krzywych z rysunku 4.103. Może się okazać, że uprzywilejowane będą stacje skrajne.



Rys. 4.103. Średnie opóźnienie ramek w buforach lokalnych stacji w funkcji numeru stacji dla wiadomości jednosegmentowych i pojedynczych rezerwacji szczelin QA

#### 4.2.9.8 Zapewnienie sprawiedliwego dostępu do medium

Opisane powyżej zjawisko nierównoprawnego (tj. niesprawiedliwego) traktowania stacji w dostępie do medium pogłębia się przy wzroście zarówno obciążenia sieci, jak też jej rozmiarów. Okazuje się bowiem, że dla sieci miejskich o znacznych rozmiarach i stosujących duże szybkości transmisji (np. rzędu 155 Mb/s) istotny wpływ na pracę stacji i całej sieci zaczynają odgrywać opóźnienia propagacyjne. Przy powyższych warunkach (tj. relatywnie dużych opóźnieniach w propagacji szczelin) kolejność otrzymywania wolnych szczelin przez oczekujące na nie stacje jest zależna nie tylko od chwili wygenerowania zgłoszenia, ale

również od fizycznego położenia stacji wzdłuż magistrali. Jeżeli, tak jak na początku rozważań, przyjmiemy możliwość wykorzystania tylko jednego bitu pola REQ do celów rezerwacji, to dla danego kierunku transmisji zdecydowanie bardziej uprzywilejowane będą stacje znajdujące się bliżej początku magistrali.

Problem zapewnienia sprawiedliwego dostępu do sieci DQDB, niezależnie od lokalizacji stacji wzdłuż magistrali, został częściowo rozwiązany poprzez opcjonalne wprowadzenie do standardu IEEE 802.6 mechanizmu BWB (ang. *BandWidth Balancing*) urównomierniania prawa dostępu (przydzielanej stacjom przepustowości). Przypomnijmy, że zgodnie z algorytmem QA stacja może wysłać przygotowaną do transmisji ramkę (segment wiadomości) każdorazowo, gdy licznik CD zeruje się, a bieżąca szczelina QA jest wolna. Mechanizm BWB, silnie oddziaływający na zachowanie się stacji w stanach przeciążenia sieci tj., gdy większość stacji zgłasza zapotrzebowanie na transmisje, pozwala stacji na przesyłanie segmentów jedynie przez część  $\alpha$  przydzielonych jej szczelin QA. Osiągamy to przez sztuczne zwiększenie o 1 stanu licznika RQ, po każdym m przesłanych przez stację segmentach; tym samym  $\alpha=m/(1+m)$ . Procedura BWB zmusza więc stację do przepuszczenia jednej wolnej szczeliny QA po każdym m zajętych przez nią szczelinach QA. Aby zaimplementować mechanizm BWB stacja musi zostać wyposażona w parę dodatkowych liczników, zliczających liczbę wykorzystanych przez nią szczelin QA.

Badania analityczne i symulacyjne wykazały, że mechanizm BWB wpływa stabilizującą na pracę całej sieci, a wartość parametru m, narzucona przez operatora, decyduje o szybszym lub wolniejszym dochodzeniu do stanu zrównania wszystkich stacji sieci w prawie dostępu do medium. Maksymalne średnie wykorzystanie przepustowości w sieci DQDB z aktywnym mechanizmem BWB jest przy tym, dla sieci N-węzłowej, równe

$$\text{efektywność sieci} = \frac{mN}{1 + mN}.$$

Mechanizm BWB może być stosowany opcjonalnie, a dopuszczalny zakres zmian parametru m wynosi od 1 do 64. Jako wartość zalecaną przyjmuje się m=8. Standard zaleca też korzystanie z mechanizmu BWB w przypadku, gdy opóźnienie propagacyjne w magistrali jest większe niż czas transmisji ramki w określonym typie medium.

#### 4.2.9.9 Metody wielokrotnego wykorzystania pojedynczej szczeliny w protokole DQDB

Możliwość wykorzystania pojedynczej szczeliny jedynie raz, w trakcie jej przebiegu wzdłuż magistrali, stanowi poważne ograniczenie protokołu DQDB. Jest to istotną przyczyną kłopotów z osiągnięciem planowanej szybkości transmisji (155 520 Mb/s - CCITT G707-9 SDH). Obecnie osiąga się szybkości: 24.686 Mb/s (CCITT G703) oraz 44 736 Mb/s (ANSI DS3). Naturalnym jest więc, że

problemowi wielokrotnego wykorzystania pojedynczej szczeliny poświęcono dużo miejsca w pracach badawczych. Obecnie można wyróżnić trzy różne metody zmierzające do tego celu:

1. Zwalnianie szczelin przez węzły, do których adresowane są segmenty - pociąga to za sobą konieczność stosowania dodatkowego wyposażenia wszystkich węzłów w mechanizm zwalniania adresowanych do nich szczelin. Każdy węzeł opóźniałby również szczelinę o co najmniej 4 oktety, tj. o czas potrzebny do zdekodowania adresu podwarstwy MAC (bądź odtworzenia identyfikatora MID);
2. Przechwytywanie wolnej szczeliny zanim zostanie ona zajęta przez stację, która ją zerezerwowała - mechanizm ten umożliwia zajęcie wolnej ramki przez stację, bez wcześniejszego wysłania rezerwacji, pod warunkiem, że adresatem wiadomości jest stacja będąca jednym z najbliższych sąsiadów danego węzła (musi leżeć przed stacją, która zarezerwowała daną szczelinę). Wprowadza to konieczność wyróżnienia w sieci DQDB klas sąsiadów, które będą rozpoznawane przez odpowiednie kombinacje wolnych bitów w polu ACF. Oprócz tego szczelina musi być opóźniona w każdym węźle o 1 oktet, potrzebny do analizy pierwszego bajtu w nagłówku ramki. W takim rozwiążaniu transmisja według zmodyfikowanego protokołu odbywa się tylko wtedy, jeżeli pakiet adresowany jest do jednego z sąsiadów (w tej samej klasie). Natomiast transmisje segmentów pomiędzy stacjami nie będącymi sąsiadami odbywają się zgodnie z klasycznym protokołem DQDB. Metoda ta przynosi pewne zyski w przypadku sieci, w których wysoki jest poziom ruchu lokalnego (pomiędzy sąsiadami w obrębie jednej klasy).
3. Wprowadzenie specjalnych węzłów (węzłów wymazujących) posiadających możliwość zwalniania tych szczelin, które służyły do przesyłania ramek/segmentów odebranych już przez adresatów. Zastosowanie tej metody nie wymaga wprowadzania istotnych zmian w działaniu normalnych węzłów. Należy zauważyć, że wprowadzenie węzłów wymazujących, bez dodatkowych modyfikacji standardowej wersji protokołu DQDB, nie wpływa jednakże na zwiększenie przepustowości sieci. Wynika to z faktu, że transmisja ramki musi być zawsze poprzedzona nadaniem żądania rezerwacji ramki. Aby było możliwe zwiększenie wykorzystania sieci, konieczne jest wprowadzenie mechanizmu zmniejszania rozproszonej kolejki żądań w zależności od liczby ramek zwolnionych przez węzły wymazujące. W standardzie przewiduje się możliwość wykorzystania bitu PSR z pola ACF do sygnalizacji, czy segment znajdujący się w szczelinie dotarł już do swojego adresata czy też nie. Jeżeli stacja rozpozna adresowany do niej segment, wówczas powinna ustawić bit PSR na 1 w szczelinie następnej. Z kolei każdy węzeł kasujący opóźnia ciąg transmitowanych bitów o nieco więcej niż

jedną szczelinę. Oznacza to, że po stwierdzeniu przez węzeł kasujący w nagłówku szczeliny k-tej bitu PSR=1 węzeł ten zmienia wartość PSR ponownie na 0 i jednocześnie zeruje zawartość, znajdującą się ciągle w buforze węzła, szczeliny (k-1)-szej - zwalniając tym samym szczelinę wykorzystaną już wcześniej do transmisji.

## 5 Bezprzewodowe sieci LAN i systemy satelitarne VSAT

Zarówno sieci radiowe jak też sieci satelitarne wykazują specyficzne cechy wynikające głównie z własności stosowanego kanału. Stanowią one alternatywę dla istniejących już sieci przewodowych. *W wielu zastosowaniach nie jest możliwe lub ekonomicznie uzasadnione tworzenie sieci komunikacyjnych z wykorzystaniem tradycyjnych mediów transmisyjnych. Możliwość obsługi stacji ruchomych i oferowanie przez radiowe sieci LAN (RLAN) jakości obsługi użytkowników na poziomie zbliżonym do gwarantowanego przez sieci przewodowe jest jednym z czynników decydujących o ich stale rosnącej popularności.* Rozsiewczy charakter transmisji w kanale radiowym umożliwia:

- łatwy dostęp do kanału i zasobów sieci poszczególnym jej użytkownikom;
- gromadzenie i rozsyłanie informacji w ramach sieci stacji końcowych rozproszonych na dużym obszarze (niezależnie od istniejących sieci przewodowych);
- możliwość komunikacji z (pomiędzy) użytkownikami ruchomymi;
- tworzenie sieci globalnych z wykorzystaniem transponderów satelitarnych.

Radiowe sieci teleinformatyczne wykazują też szereg innych pozytywnych własności jak: łatwość rozbudowy, duża niezawodność, stosunkowo niski koszt tworzenia sieci.

Wśród ich zasadniczych wad należy wymienić stosunkowo duże rozpraszczenie energii (z uwagi na mały promień jej koncentracji), wysoki poziom zakłóceń zewnętrznych (spowodowany małą kierunkowością anten odbiorczych), łatwość dostępu nieautoryzowanego (podsłuch) oraz możliwość celowego zakłócania transmisji.

Gdy ograniczone zasoby są użytkowane przez dużą liczbę niezależnych użytkowników pojawia się każdorazowo potrzeba stosowania protokołów wielodostępu. W kolejnych paragrafach omówimy zarówno popularne algorytmy ALOHA i CSMA, nie będące standardami, jak też standardowe propozycje organizacji dostępu do medium IEEE 802.11 i ETSI HIPERLAN, zyskujące coraz szersze zastosowanie. Dwa pierwsze paragrafy, poświęcone omówieniu prostych algorytmów ALOHA i CSMA dla sieci bezprzewodowych, mogą być traktowane jako wprowadzenie do omawianego w poprzednim rozdziale najpopularniejszego standardu sieci LAN jakim jest CSMA/CD IEEE 802.3. W ostatnim paragrafie rozdziału omówione zostaną podstawowe własności i zastosowania sieci typu VSAT.

### 5.1 Sieć i protokół dostępu ALOHA

Sieć komputerowa ALOHA jest pierwszą radiową siecią teleinformatyczną, tj. siecią wykorzystującą radiowe medium propagacyjne do transmisji danych i stosującą komutację pakietów. Struktura sieci, opracowanej i wdrożonej na Uniwersytecie Hawajskim w 1970 r., jest skoncentrowana, a jej topologia drzewiasta. Sieć składa się z:

- centrum komputerowego, w którym w chwili inicjowania pracy sieci zainstalowany był komputer IBM 360/65;
- komputera stykowego (ang. *front-end-computer*); HP 2115A;
- odległych jednostek dwóch typów:
  - prostych terminali (ang. *Terminal Control Unit - TCU*) pracujących w systemie półduplekowym i wyposażonych w bufor, jednostkę sterującą oraz modem radiowy;
  - systemów mikroprocesorowych (ang. *Packet Control Unit - PCU*) służących do koncentracji danych z TCU.

Do komunikacji stacji końcowych (przyłączonych do sieci za pośrednictwem TCU lub PCU) z centrum wykorzystywane są dwa wydzielone podkanały łączności:

k1 - o częstotliwości  $f_1 = 405.35$  MHz, do transmisji ramek z węzłów PCU i TCU do centrum oraz

k2 - o częstotliwości  $f_2 = 413.475$  MHz, do transmisji ramek z węzła centralnego do TCU i PCU. Oba kanały mają pasma o szerokości po 100 kHz, a do transmisji sygnałów stosowana jest modulacja PSK. Szybkość transmisji wynosi przy tym 24kb/s.

W celu zwiększenia zasięgu pracy w sieci stosowane są stacje przekaźnikowe realizujące komutację pakietów (ang. *store-and-forward, packet switching*).

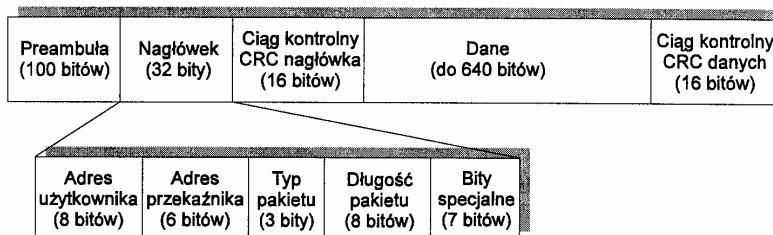
#### 5.1.1 Formaty ramek

W systemie ALOHA przesyłane są dwa typy ramek: ramki informacyjne (o dwóch podstawowych długościach) oraz powiadomienia pozytywne ACK. Wszystkie ramki rozpoczynają się preambułą (100 bitów) służącą do synchronizacji pracy nadajników i odbiorników stacji końcowej i centralnej (bądź przekaźnika). Kolejne pola ramek (w tym ACK) tworzą nagłówek. Obejmuje on:

- adres użytkownika (8 bitów),
- adres przekaźnika (3 bity),
- długość pola danych ramki (8 bitów-reprezentujących liczbę bajtów),
- specjalne bity kontrolne (3 bity).

Nagłówek ramki informacyjnej lub ACK zabezpieczony jest 2-bajtowym ciągiem CRC. Ramki informacyjne mogą posiadać pole danych o długościach do

40-stu lub 80-ciu bajtów (320 lub 640 bitów). Pole danych ramki informacyjnej zabezpieczone jest, podobnie jak nagłówka, ciągiem CRC o długości 2-ch bajtów. Ilustruje to rys. 5.1.



Rys. 5.1. Struktura ramki informacyjnej w protokole ALOHA (w sieci ALOHA)

### 5.1.2 Algorytmy dostępu ALOHA i zasady wymiany informacji w sieci ALOHA

ALOHA jest najwcześniej opracowanym algorytmem swobodnego dostępu do propagacyjnego medium radiowego. Wykorzystanie protokołu nie musi jednakże ograniczać się do kanału radiowego, lecz może być rozszerzone na dowolne media propagacyjne. Należy podkreślić, że koncepcja niekontrolowanego dostępu, sformułowana w algorytmie ALOHA, znalazła swoje rozwinięcie w rodzinie protokołów CSMA, CSMA/CD i wielu innych.

W przypadku reguły dostępu ALOHA stacja końcowa mająca, ramkę przygotowaną do transmisji i zgromadzoną w buforze nadajnika, wysyła ją bez jakiegokolwiek opóźnienia i bez koordynacji działań z innymi stacjami. Kopia wysłanej ramki wprowadzana jest do bufora kopii, gdzie pozostaje do chwili odbioru powiadomienia ACK; stacja przechodzi natomiast w tzw. stan blokady. Oznacza to, że niemożliwa staje się transmisja nowej ramki (stacje realizują algorytm sterowania przepływem ramek typu stop-and-wait). Czas oczekiwania na powiadomienie (time-out) uwzględnia opóźnienia propagacyjne na trasie stacja końcowa-centrum oraz opóźnienia wnoszone przez przekaźniki. W przypadku braku odbioru powiadomienia ACK przed upływem time-out-u realizowana jest procedura retransmisji ramki. Aby uniknąć wielokrotnych kolizji tych samych ramek, stacja określa tzw. przedział randomizacji retransmisji, nazywany też oknem retransmisji (przedział ten jest zwykle znacznie większy od czasu transmisji pojedynczej ramki), i dokonuje losowego wyboru chwili rozpoczęcia kolejnej próby dostępu do medium w ramach tego okna. Przyczyną braku napłygnięcia ACK mogą być przy tym zarówno błędy interferencyjne, jak też błędy spowodowane szumem w kanale.

Zgodnie z procedurami pracy stacji końcowych i węzła centralnego w sieci ALOHA protokół swobodnego dostępu ALOHA stosowany jest w kanale k1.

Poszczególne stacje rywalizujące o dostęp przesyłają ramki informacyjne bez wzajemnej koordynacji, tj. bez uwzględnienia jakiegokolwiek dodatkowej informacji pomocniczej o stanie kanału/sieci.

Kanał k2 jest wykorzystywany do bezkolizyjnego przesyłania dwóch typów ramek: powiadomień pozytywnych ACK oraz ramek informacyjnych (z danymi) z węzła centralnego. Ramki ACK mają przy tym bezwzględny priorytet przed ramkami danych. Ramki informacyjne są transmitowane jedynie wtedy, gdy kolejka ACK jest pusta. Ramki informacyjne przesyłane kanałem k2, do stacji końcowych, nie są powiadamiane oddzielnymi ramkami ACK. Przyjęto bowiem, że ich transmisje są praktycznie bezbłędne (są one przesyłane bezinterferencyjnie, a ewentualne straty ramek ACK są wykrywane przez protokoły warstw wyższych). Zauważmy, że wysyłanie dodatkowych ramek ACK spowodowałoby zwiększyły ruch w kanale k1 i wzrost prawdopodobieństwa kolizji.

W celu zwiększenia zasięgu pracy w sieci stosowane są stacje przekaźnikowe realizujące komutację pakietów. Prekaźniki wykorzystują kanały k1 i k2. Każdy z nich posiada listę adresów ewentualnych innych przekaźników (węzłów pośredniczących), z którymi może się komunikować. Węzeł centralny nie może nadawać na częstotliwości  $f_2$  kanału k2 w tym samym czasie co przekaźnik, ponieważ stacje leżące w zasięgu przekaźnika i węzła centralnego (od dwóch kolejnych przekaźników) odbierałyby interferującą ramkę. Po każdej transmisji ramki węzeł musi czekać przez pewien czas, by przekaźnik zdążył zrealizować retransmisję.

Istotnym elementem w pracy sieci ALOHA jest kierowanie ruchem ramek/pakietów. W pierwszej wersji tej sieci przyjęto stałe trasy przesyłania ramek, przy jednoczesnym zapewnieniu unikatowych adresów poszczególnych przekaźników.

### 5.1.3 Uproszczona analiza jakości protokołu ALOHA

Dokonamy tutaj uproszczonej analizy jakości protokołu ALOHA. Przedmiotem tej analizy będzie ocena wykorzystania kanału k1 w sieci ALOHA. Założymy przy tym, że:

- strumień zgłoszeń ramek (nowych i retransmitowanych) wprowadzanych do k1 przez wszystkie stacje końcowe jest poissonowski, o intensywności  $g$  ramek na sekundę,
- liczba stacji końcowych  $N$  jest bardzo duża (teoretycznie  $N \rightarrow \infty$ ),
- czasy transmisji wszystkich ramek informacyjnych są jednostkowe ( $T=1$ ),
- jedną przyczyną retransmisji ramek są interferencje,
- topologia sieci jest gwiazdzista (założenie to nie ma przy tym żadnego wpływu na efektywność protokołu).

Założenia powyższe nie opisują wiernie zachowania się rzeczywistego systemu ALOHA. Umożliwiają jednakże otrzymanie związków zależności analitycznych,

pozwalających na zgrubną ocenę efektywności protokołu. Efektywność protokołu opisywać będziemy przy tym trzema parametrami: średnim przepływem  $S$ , średnią zajętością kanału  $G$  i średnim czasem opóźnienia  $D$  przy transmisji ramek. Przyjmując poissonowski strumień zgłoszeń o intensywności  $g$  i jednostkowy czas  $T$  trwania ramek informacyjnych, średnią zajętość  $G$  kanału (całkowity ruch oferowany przez wszystkie stacje sieci) możemy opisać jako:

$$G = gT = g[\text{ramek/s}]_{T=1}.$$

Na całkowity ruch w sieci składają się dwa składniki: ramki przesypane po raz pierwszy i retransmitowane. W warunkach równowagi pracy sieci prawdziwa jest przy tym zależność:

$$G = S + GP_r \quad (\text{retransmisi},$$

gdzie  $S$  jest średnią liczbą ramek nowych, wprowadzanych do  $k_1$  w czasie jednostkowym.

Biorąc pod uwagę założenie o poissonowskim strumieniu zgłoszeń oraz przyjęcie, że jedyną przyczyną błędów (i retransmisi) są interferencje ramek, prawdopodobieństwo  $P_r$ (retransmisi) jest równe:

$$\Pr(\text{retransmisi}) = 1 - \exp(-2G).$$

We wzorze powyższym składnik  $\exp(-2G)$  reprezentuje prawdopodobieństwo braku interferencji wybranej ramki z jakąkolwiek inną. Prawdopodobieństwo to opisuje brak rozpoczęcia się jakąkolwiek transmisji ramki (z wyjątkiem wybranej) w przedziale czasu o długości równej podwojonymu czasowi transmisji ramki; ilustruje to rysunek 5.2a.

Ostatecznie średni przepływ, tj. średnia liczba ramek udanie transmitowanych w kanale  $k_1$  w czasie jednostkowym (równa w warunkach równowagi średniej liczbie ramek nowogenerowanych w czasie  $T=1$ ) wynosi:

$$S = Ge^{-2G}.$$

Maksymalna wartość  $S$  jest natomiast równa:

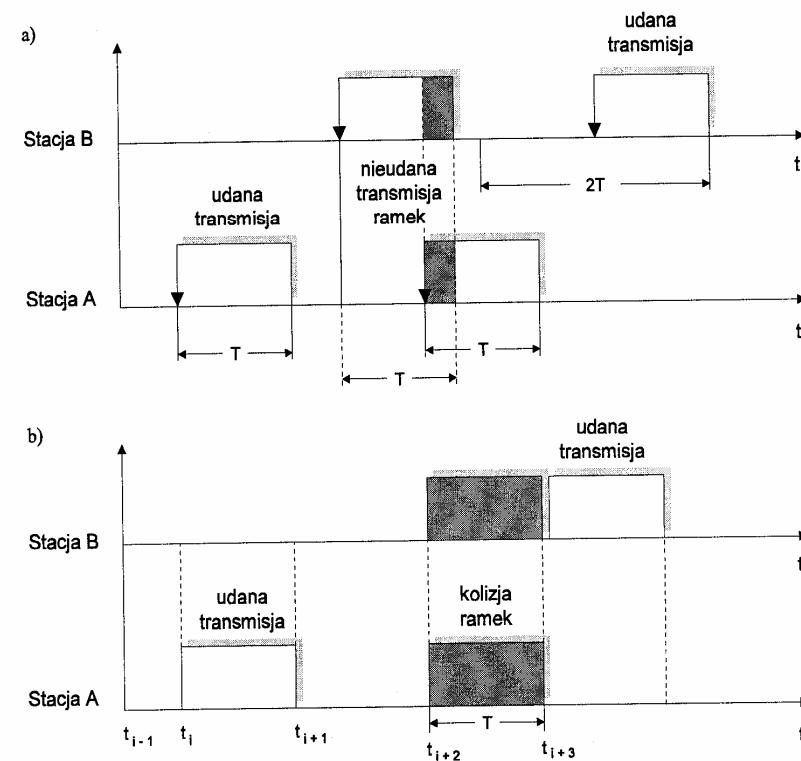
$$S_{\max} = \max_G S = \frac{1}{2e} \Big|_{G=0.5} \approx 0.184.$$

Z kolei opóźnienie  $D$  przy transmisji ramek między stacją końcową, a centrum możemy opisać jako:

$$D = \left( \frac{G}{S} - 1 \right) \left( 1 + 2a + w + \frac{K+1}{2} \right) + a + 1$$

gdzie:

$\frac{G}{S}$	- stanowi średnią liczbę retransmisji pojedynczej ramki informacyjnej,
$a$	- jest tzw. znormalizowanym opóźnieniem propagacyjnym w kanale ( $k_1$ lub $k_2$ ),
$w$	- stanowi czas potrzebny na generację przez węzeł centralny powiadomienia ACK
$\frac{K+1}{2}$	- jest średnim czasem, po którym następuje retransmisja ramki; przy czym $K$ jest długością czasu randomizacji retransmisji (szerokością okna retransmisji),
$1+a$	- reprezentuje unormowany czas potrzebny na transmisję ramki do dotarcie jej do adresata.



Rys. 5.2. Przykładowe ilustracje wykorzystania kanału wspólnego w systemach z protokołami ALOHA - (a) i S-ALOHA - (b)

Zakładając, że szybkość transmisji w systemie ALOHA wynosi 24 kb/s, to czas transmisji pojedynczej ramki informacyjnej składającej się z 704 bitów będzie równy 29 ms. Jeżeli dodatkowo uwzględnimy typowy 5 ms ciąg synchronizacyjny poprzedzający ramkę, to łączny czas T zajętości kanału wyniesie 34 ms. Przyjmując dalej, że nowe ramki są generowane i transmitowane przez każdą ze stacji z intensywnością  $\lambda_1 = 1/60$  [1/s] (czyli co 1 minutę), wówczas maksymalne obciążenie kanału ramkami nowogenerowanymi możemy wyrazić zależnością:

$$S_{\max} = N_{\max} \lambda_1 T \approx \frac{1}{2e}.$$

Tym samym średnią maksymalną liczbę  $N_{\max}$  czynnych stacji, współużytkujących kanał, możemy w przybliżeniu wyznaczyć jako:

$$N_{\max} \approx \frac{1}{2\lambda_1 T e} \approx 320.$$

#### 5.1.4 Założenia ogólne i jakość protokołu S-ALOHA

Maksymalny średni przepływ,  $S_{\max}$ , w kanale k1 sieci ALOHA stanowi jedynie około 18% teoretycznej przepustowości ( $C=1$ ) kanału. W celu poprawienia efektywności protokołu, w pracy sieci i stacji końcowych wprowadzono pewne modyfikacje. Polegają one między innymi na podziale czasu pracy kanału na szczeliny czasowe (ang. *slots*) o długości w przybliżeniu równej czasowi transmisji ramki informacyjnej (gdy pominiemy opóźnienia propagacyjne). Algorytm pracy stacji realizujących zmodyfikowany protokół ALOHA, tzw. protokół S-ALOHA (ang. *Slotted ALOHA*) jest wówczas następujący:

- Ramka wygenerowana przez źródło informacji obsługiwane przez TCU w szczelinie  $i-1$ , czyli w przedziale czasu  $(t_{i-1}, t_{i-1}+1)$ , jest wprowadzana do bufora TCU (o ile jest on pusty - stacja nie jest zablokowana) i wysyłana w chwili  $t_i$  ( $t_i = t_{i-1} + 1$ ) poczynając kolejną szczelinę o jednostkowym czasie trwania (zgodnie z założeniami przyjętymi dla algorytmu ALOHA).
- Jeżeli ramka nie zostaje potwierdzona przed upływem time-out-u, stacja (i ramka) przechodzi w stan blokady. Następuje retransmisja ramki w przedziale randomizacji. W czasie blokady może mieć miejsce jedynie retransmisja ramki przechowywanej w buforze stacji.

Rozważenia analogiczne do prowadzonych w poprzednim paragrafie pozwalają na wyznaczenie średniego przepływu  $S$  w kanale k1, w przypadku stosowania reguły dostępu S-ALOHA. Wartość  $S$  jest w tym przypadku równa:

$$S = Ge^{-G}.$$

Proste rozważania optymalizacyjne pozwalają na wyznaczenie  $S_{\max}$ :

$$S_{\max} = \max_G S = \left. \frac{1}{e} \right|_{G=1} \approx 0.37.$$

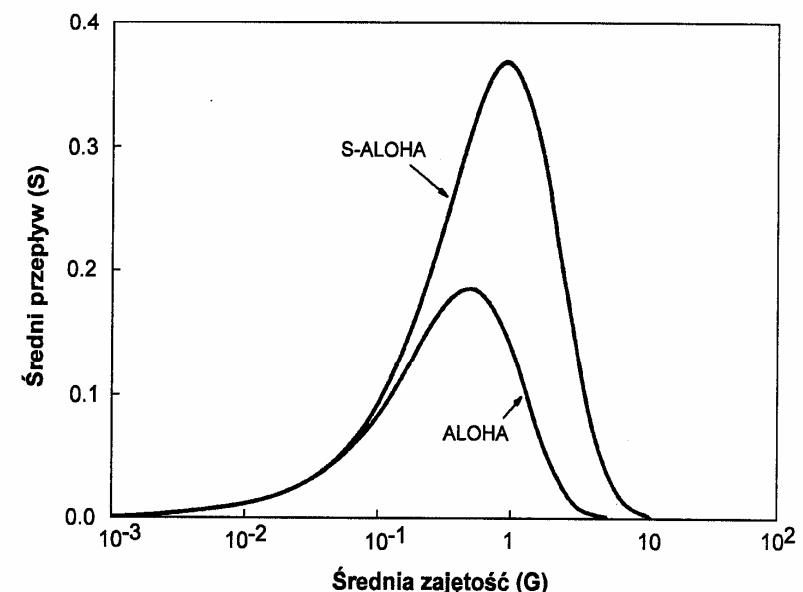
Tym samym okazuje się, że wprowadzenie dyskretyzacji chwil inicjowania transmisji przez stacje pozwala na dwukrotny wzrost  $S_{\max}$  w stosunku do wartości uzyskanej dla protokołu ALOHA. Wynika to z ograniczenia możliwości wystąpienia interferencji ramek poprzez dwukrotne zawężenie okna interferencji (patrz rysunek 5.2b).

Z kolei średnie opóźnienie przy transmisji ramki ze stacji końcowej do centrum wynosi:

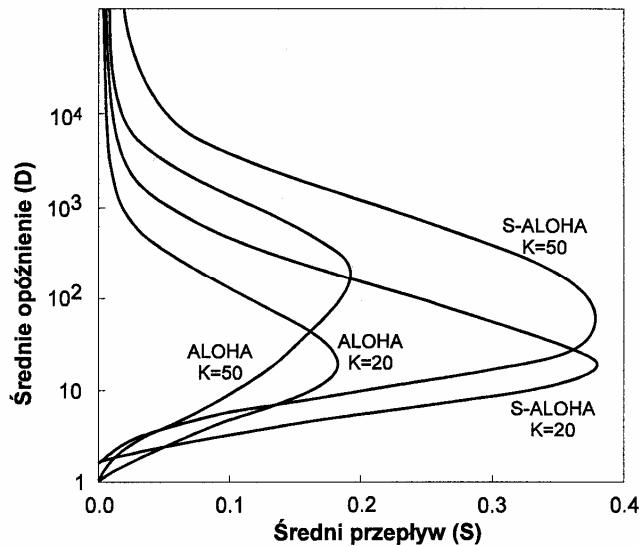
$$D = (\exp G - 1) \left( 1 + 2a + \frac{K+1}{2} \right) + 1.5a + 1.5.$$

Wzrost wartości dwóch ostatnich składników wiąże się z koniecznością dłuższego przebywania ramki informacyjnej (bądź ACK) w buforze stacji (centrum) przed transmisją.

Porównanie zmian  $S = f(G)$  oraz  $D = f(S)$  przedstawiono na rysunkach 5.3 i 5.4.



Rys. 5.3. Zmiany średniego przepływu  $S$  w funkcji zmian zajętości  $G$  kanału wspólnego dla protokołów ALOHA i S-ALOHA



Rys. 5.4. Zmiany opóźnienia D przy zmianach średniego przepływu S dla protokołów ALOHA i S-ALOHA

### 5.1.5 Uwagi na temat stabilności protokołów typu ALOHA

Z teoretycznego punktu widzenia, cechą charakterystyczną pracy sieci stosujących algorytm typu ALOHA jest ich niestabilność (uwaga ta dotyczy wszystkich algorytmów z rywalizacją stacji o dostęp do medium propagacyjnego). Przy pewnych warunkach związanych z nadmierną intensywnością napływu pakietów do kanału, rosną bardzo szybko (lawinowo) liczby ramek interferujących (przyjmując  $N \gg 1$ , a w szczególności  $N \rightarrow \infty$ ), a tym samym i kolejki ramek oczekujących na retransmisję. Rodzi się więc pytanie, kiedy możemy oczekiwać pojawienia się niestabilności oraz jakie miary tego zjawiska możemy przyjąć. Ażkolwiek zagadnienie stabilności nie jest przedmiotem naszego szczególnego zainteresowania w niniejszej pracy, to z uwagi na decydujący wpływ tego zjawiska na dynamikę pracy sieci należy na nie zwrócić uwagę. Stabilność systemu z protokołem ALOHA może być definiowana następująco: *System ten jest stabilny, gdy nowe ramki generowane przez stacje końcowe tworzą wejściowy proces odnowy, a intensywność sumarycznego strumienia wejściowego  $\lambda$  jest mniejsza od  $1/e$ .* Podobnie możemy sformułować warunek stabilności dla systemu S-ALOHA, tzn.  $\lambda < 1/e$ . Ogólnie stabilność systemu wiąże się jednoznacznie z gwarantowaną przez system intensywnością obsługi ramek. Jeżeli intensywność ta jest większa od intensywności napływu informacji, to możemy oczekивать stabilnej pracy systemu.

W rozważanych dotychczas modelach zakładaliśmy, że sumaryczny strumień zgłoszeń do wspólnego kanału jest poissonowski. Z założenia tego wynikało między innymi to, że rozkład czasu zarówno pomiędzy kolejnymi próbami retransmisji jak też pomiędzy udaną transmisją, a generacją kolejnego nowego zgłoszenia, był wykładniczy o identycznym parametrze  $g$ . Tymczasem w rzeczywistych systemach średni czas poprzedzający generację nowej ramki (tzw. czas myślenia) jest zwykle inny niż średni czas pomiędzy kolejnymi próbami retransmisji. Z probabilistycznego punktu widzenia inne więc będą prawdopodobieństwa podejmowania prób transmisji i retransmisji w kolejnych np. szczelinach czasowych w systemie S-ALOHA. W systemach ze sterowaniem przepływem ramek typu SAW ma miejsce blokada stacji, tj. zakaz wysyłania nowych ramek - do chwili udanej transmisji ramki aktualnie obsługiwanej. W przypadku stacji pracujących nierytmicznie może dojść do sytuacji, gdy na skutek dużej intensywności zgłoszeń nowych ramek i ich wzajemnych interferencji większość ze stacji znajdzie się w stanie blokady. Jeżeli prawdopodobieństwa retransmisji w tym stanie będą zbyt duże, to kolejne próby nadawania ramek mogą ten stan pogłębić, prowadząc w skrajnym przypadku do całkowitej blokady systemu. Wynika stąd wniosek, że prawdopodobieństwa retransmisji ramek muszą być tak dobrane, aby pozwalały na rozładowywanie stanów blokady stacji. Jednocześnie intensywności zgłoszeń nie mogą przekraczać znormalizowanej przepustowości systemu ( $S_{\max}$ ).

## 5.2 Algorytmy dostępu typu CSMA i ich przykładowa implementacja

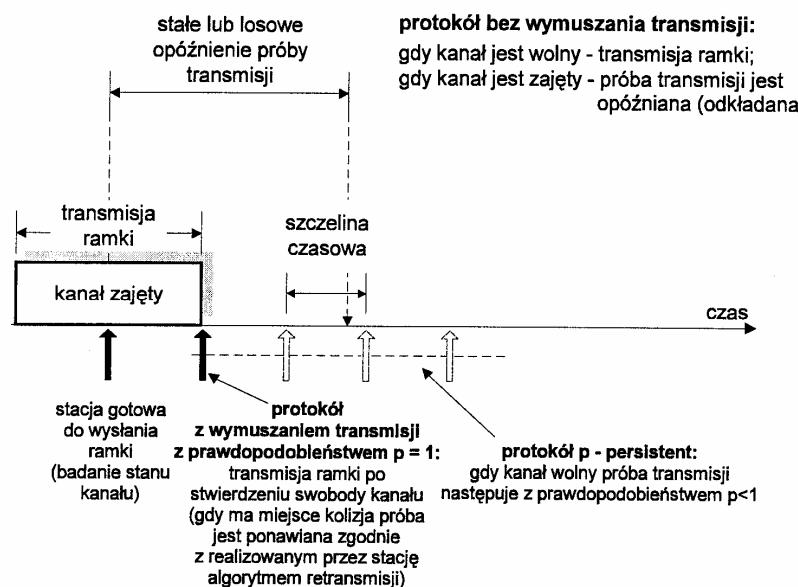
Niewątpliwą zaletą opisanych poprzednio algorytmów typu ALOHA jest duża prosta ich funkcjonowania. Wadą tych algorytmów jest jednakże niewielka sprawność wykorzystania kanału, nie przekraczająca 37% w przypadku protokołu S-ALOHA. Jest ona ceną jaką płacimy za to, że przy realizacji dostępu do medium stacje wykorzystują minimalną ilość informacji pomocniczej o stanie kanału. Wzrost ilości informacji pomocniczej, którą dysponują stacje, może wydatnie zwiększyć efektywność ich funkcjonowania. W przypadku szerokiej klasy protokołów typu CSMA (ang. *Carrier Sense Multiple Access*) informację tę uzyskujemy poprzez śledzenie nośnej w kanale (ang. *carrier sense*).

### 5.2.1 Zasady funkcjonowania algorytmów ze śledzeniem nośnej - CSMA

Wśród algorytmów CSMA wyróżniamy algorytmy szczelinowe (ang. *slotted*), charakteryzujące się możliwością wprowadzania ramek do kanału jedynie w ściśle określonych chwilach czasu, oraz algorytmy bezszczelinowe, tj. bez wyróżnionych chwil wprowadzania informacji do medium.

We wszystkich typach algorytmów CSMA transmisja ramki musi być poprzedzona badaniem stanu kanału. Jedynie wtedy, gdy w kanale nie zostaje wykryta żadna transmisja (brak sygnału), stacja może podjąć próbę transmisji. Wyróżniamy przy tym algorytmy:

- CSMA bez wymuszania transmisji (ang. *nonpersistent*): w tym przypadku stacja, która ma ramkę gotową do transmisji, po stwierdzeniu zajętości kanału rezygnuje chwilowo z realizacji transmisji, dokonując losowania przedziału czasu, po którym ponawia próbę dostępu, zgodnie z ilustracją pokazaną na rysunku 5.5.



Rys. 5.5. Protokoły CSMA bez wymuszania transmisji (*nonpersistent*) i z wymuszaniem transmisji z prawdopodobieństwem  $p$  ( *$p$ -persistent*)

- CSMA z wymuszaniem transmisji z prawdopodobieństwem  $p$  (ang.  *$p$ -persistent*): w tej wersji algorytmu użytkownik mający ramkę przygotowaną do transmisji, po stwierdzeniu zajętości kanału, czeka do momentu "zwolnienia" kanału, po czym dokonuje dyskretyzacji czasu na szczeliny o długości równej podwojnemu maksymalnemu opóźnieniu propagacyjnemu w sieci i z prawdopodobieństwem  $p$  ( $p \in (0,1)$ ) dokonuje próby (lub z  $1-p$  zaniechania) transmisji w kolejnych szczelinach (śledząc przez cały czas stan kanału). Postępowanie to ilustruje rysunek 5.5.

### 5.2.2 Przykładowa implementacja protokołu CSMA

Algorytm CSMA (będący pierwowzorem CSMA/CD) znajduje dość szerokie zastosowanie praktyczne; jest na przykład wykorzystywany jako protokół dostępu do medium, tj. algorytm podwarstwy MAC, w pakiecie oprogramowania AX.25 stanowiącym radioamatorską wersję standardu X.25 dla pakietowej sieci publicznej.

Inny przykład implementacji CSMA stanowi radiowa sieć MP-NET zrealizowana na terenie Montrealu. W sieci tej stacje pracują na jednej częstotliwości 223.050 MHz z niewielką szybkością transmisji 4800 b/s, stosując modulację FSK. Sieć jest zorganizowana w grupy stacji połączonych przekaźnikami. Każdy z nich posiada rozłączne zbiory adresów dla grup stacji, które łączy. Stacje posiadają specjalne tablice, pozwalające im określić przynależność adresata do tej samej lub innej grupy i w razie potrzeby - przesyłać ramkę do odpowiedniego przekaźnika.

Stosowane w tej sieci ramki mają zunifikowaną postać i stosują znaki/pola o podanym poniżej znaczeniu:

- SYN SYN (2 bajty) - znaki synchronizacji,
- SOH (1 bajt) - znak początku nagłówka,
- pole długości (1 bajt) - długość ramki w bajtach (bez początkowych znaków sterujących),
- pole adresu stacji docelowej (6 bajtów) - adresat może znajdować się w tej samej grupie, co nadawca, lub też innej grupie stacji,
- adres przekaźnika docelowego (1 bajt) - określa numer przekaźnika obsługującego stację docelową,
- adres stacji źródłowej (6 bajtów),
- adres przekaźnika źródłowego (1 bajt),
- kolejny numer ramki (1 bajt) - określa numer ramki w przesyłanym ciągu ramek; (0,...,255),
- status ramki (1 bajt) - określa typ ramki:  
A - ACK,  
R - ramka retransmitowana przez przekaźnik,  
F - ramka numerowana będąca częścią transmitowanego pliku,  
B - binarne pole danych (a nie ASCII),  
E - inne niż binarne bądź ASCII pole danych.
- pole zarezerwowane (1 bajt) - z przeznaczeniem do wykorzystania w przyszłości,
- dane (0 - 236 bajtów),
- CRC (2 bajty) - ciąg kontrolny kodu cyklicznego.

W przypadku powyższej sieci, ramki ACK stosowane są wyłącznie do pozytywnego powiadomiania stacji źródłowej o udanym przekazaniu ramek informacyjnych. W ramkach ACK pole danych ma zerową długość.

Przesyłanie ramki do innej grupy stacji przebiega w sposób następujący:

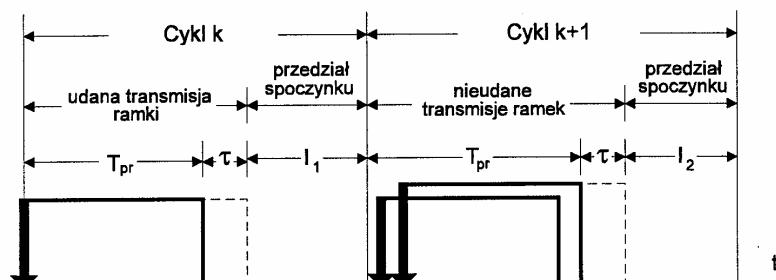
- Przekaźnik ignoruje wszystkie ramki, które mają puste pola adresowe przekaźnika;
- Jeżeli pole przekaźnika zawiera właściwy adres, wówczas sprawdza on czy adres przeznaczenia jest poprawny, ustawia status ramki na R, wyznacza nowe CRC i retransmituje ramkę;
- Stacja końcowa ignoruje wszystkie te ramki, które mają wypełniony adres przekaźnika, a nie posiadają statusu R. W ten sposób unika się ewentualnego dwukrotnego odbioru tej samej ramki (od stacji źródłowej i od przekaźnika);
- Pole adresowe przekaźnika źródłowego wykorzystywane jest do przesyłania powiadomienia ACK w kaskadowych połączeniach przekaźników.

### 5.2.3 Wybrane wyniki analizy algorytmów CSMA

Protokoły CSMA pozwalają w sposób istotny poprawić efektywność wykorzystania medium wielodostępnego, poprzez poprzedzenie transmisji ramek badaniem stanu kanału. Ich parametry jakościowe zależą jednakże w sposób bardzo silny od znormalizowanych opóźnień propagacyjnych  $\tau/T$  między stacjami sieci (gdzie  $\tau$  - opóźnienie propagacyjne, a  $T$  - czas transmisji ramki).

Przy wzroście stosunku  $\tau/T$  do wartości 1, korzyści, wynikające ze śledzenia nośnej w kanale, maleją do zera tzn. jakość protokołu CSMA staje się identyczna z jakością protokołów ALOHA, bądź S-ALOHA, w zależności od wersji CSMA, a dla  $\tau/T > 1$  jakość protokołu CSMA staje się gorsza niż uzyskiwana w przypadku algorytmów ALOHA bądź S-ALOHA, w zależności od sposobu wprowadzania ramek do kanału.

Prowadząc obserwacje stanu kanału zauważamy cyklicznie powtarzające się okresy pracy stacji (udane lub nieudane transmisje ramek) oraz przedziały spoczynku (bezczynności stacji), zgodnie z ilustracją podaną na rysunku 5.6.



Rys. 5.6. Ilustracja pracy kanału w systemie z protokołem CSMA

Jeżeli założymy, że:

- zgłoszenia oferowane do kanału (udane/nieudane re/transmisje ramek oraz próby dostępu) tworzą proces Poissona o intensywności  $g$  (zgłoszeń (prób))/ sekundę),
- opóźnienia propagacyjne  $\tau$  między stacjami sieci są jednakowe, a
- czasy transmisji ramek są równe  $T$ ,

wówczas całkowity ruch,  $G$ , oferowany do kanału możemy zapisać jako

$$G=gT.$$

Biorąc pod uwagę powyższe założenia średni przepływ  $S$  możemy przedstawić w postaci ogólnej, jako

$$S = \frac{TP_r(\text{udane transmisji})}{\bar{T}_{pr} + \bar{I}},$$

gdzie

$\bar{T}_{pr}$  - jest średnią długością okresu zajętości (pracy) kanału ramkami udane/nieudane re/transmitowanymi przez stacje,

$\bar{I}$  - jest średnią długością czasu spoczynku (przerwy) w pracy wszystkich stacji,

$\bar{T}_{pr} + \bar{I}$  - jest średnią długością cyklu pracy kanału.

Dokonując stosownej analizy długości cykli pracy w różnych wersjach algorytmu CSMA otrzymujemy następujące wartości średniego przepływu  $S$  wyrażone w funkcji ruchu oferowanego  $G$ .

#### Algorytmy bezszczelinowe

##### CSMA bez wymuszania transmisji

$$S = \frac{Ge^{-aG}}{G(1+2a) + e^{-aG}}$$

gdzie  $a = \tau/T$ .

##### CSMA z wymuszaniem transmisji z prawdopodobieństwem 1

$$S = \frac{Ge^{-G(1+2a)}[1 + G + aG(1 + G + aG/2)]}{G(1+2a) - (1 - e^{-aG}) + (1 + aG)e^{-G(1+a)}}.$$

#### Algorytmy szczelinowe

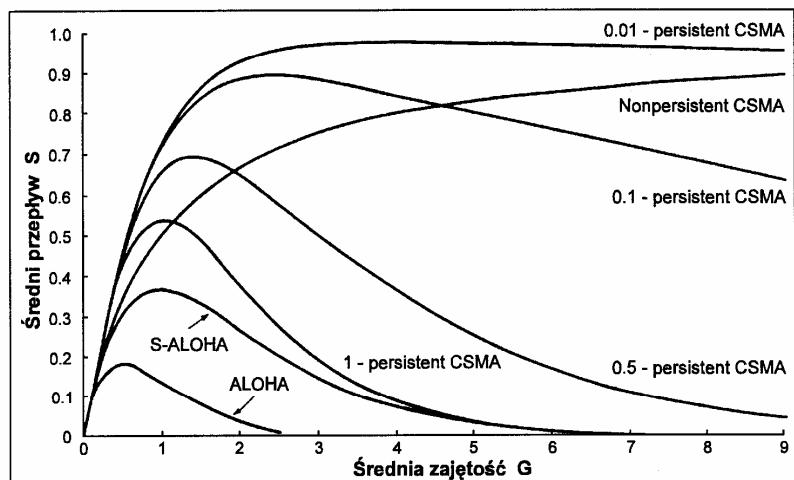
##### CSMA bez wymuszania transmisji

$$S = \frac{aGe^{-aG}}{1 + a - e^{-aG}}.$$

### CSMA z wymuszaniem transmisji z prawdopodobieństwem 1

$$S = \frac{Ge^{-(1+a)G} (1 + a - e^{-aG})}{(1+a)(1 - e^{-aG}) + ae^{-(1+a)G}}$$

Przykładowe zmiany średniego przepływu  $S$  przy zmianach  $G$  dla różnych algorytmów CSMA (przy założeniu  $a \ll 1$ ) przedstawione zostały na rysunku 5.7.



Rys. 5.7. Porównanie zmian wykorzystania kanału (średniego przepływu) w funkcji zajętości, dla różnych wersji protokołu CSMA oraz ALOHA i S-ALOHA

### 5.3 Rozproszony algorytm dostępu podwarstwy MAC dla bezprzewodowej sieci LAN

#### - Standard DFWMAC IEEE 802.11

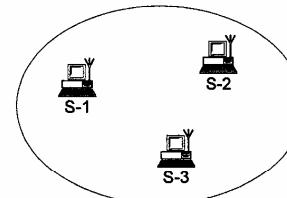
Opracowany przez IEEE standard dla bezprzewodowych sieci LAN, określany mianem *Distributed Foundation Wireless MAC (DFWMAC)*, stanowi element pełnej architektury protokolowej pozwalającej na organizację bezprzewodowego systemu LAN. Standard DFWMAC specyfikuje funkcje i zasady pracy podwarstwy MAC i warstwy fizycznej. W przypadku tej ostatniej, tj. najniższej warstwy sieci standard przewiduje kilka wersji rozwiązań, z wykorzystaniem pasm częstotliwości w zakresie GHz i stosowania metod wielodostępu kodowego z użyciem specjalnych sygnałów rozpraszających widmo (ang. DS SS - *Direct Sequence Spread Spectrum* i FH SS - *Frequency Hopping Spread Spectrum*) bądź z wykorzystaniem komunikacji na podczerwieni.

### 5.3.3 Rozproszony algorytm dostępu podwarstwy MAC dla bezprzewodowej sieci LAN...

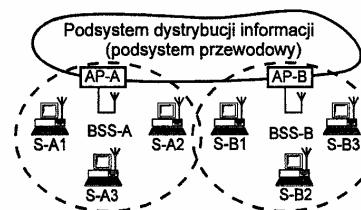
#### 5.3.1 Podstawowe cechy standardu IEEE 802.11

W oparciu o protokół DFWMAC mogą być realizowane dwa typy sieci radiowych:

- rozproszone radiowe sieci LAN (RLAN) obejmujące stacje robocze znajdujące się w zasięgu wzajemnej słyszalności i organizowane jako sieci o doraźnej, nietrwałej strukturze organizacyjnej (tzw. sieci ad hoc) pokazane na rysunku 5.8 oraz
- "wielokomórkowe" sieci radiowe, w których stacje robocze znajdujące się w różnych strefach, tzw. podstawowych obszarach obsługi BSA (ang. *Basic Service Area*), komunikują się wzajemnie za pośrednictwem wydzielonych punktów dostępu AP (ang. *Access Point*) i stałej przewodowej infrastruktury sieciowej. Przewodowa infrastruktura sieciowa stanowi podsystem dystrybucji informacji pozwalający na znaczne zwiększenie zasięgu działania sieci RLAN (patrz rysunek 5.9).



Rys. 5.8. RLAN o doraźnej, nietrwałej strukturze organizacyjnej (typu „ad hoc”)



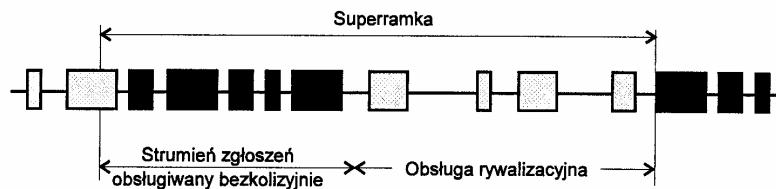
Rys. 5.9. Wielokomórkowe sieci radiowe z przewodową infrastrukturą sieciową. Oznaczenia: AP - punkt dostępu do podsieci przewodowej, S - stacja ruchoma, BSS - zespół stacji w danym podstawowym obszarze obsługi (komórce sieci)

Standard IEEE 802.11 DFWMAC specyfikuje dwie wersje algorytmów pracy stacji i sieci, związane z dwoma rodzajami usług oferowanych przez podwarstwę MAC. Algorytmy tworzące DFWMAC to:

- Algorytm z Rozproszoną Funkcją Koordynacji Dostępu DCF (ang. *Distributed Coordination Functions*) oraz

- Algorytm z Punktową Funkcją Koordynacji Dostępu PCF (ang. *Point Coordination Function*).

Algorytm DCF zapewnia obsługę ruchu asynchronicznego z wykorzystaniem metody dostępu CSMA/CA (ang. *Carrier Sense Multiple Access with Collision Avoidance*). DCF stanowi przy tym podstawową wersję pracy sieci w standardowym zestawie IEEE 802.11. Z kolei algorytm PCF pozwala na obsługę zgłoszeń (ramek) wymagających spełnienia ostrych reżimów czasowych (ruch synchroniczny z ograniczeniami narzuconymi na czas obsługi i/lub częstotliwość dostępu do kanału). Protokół PCF jest realizowany opcjonalnie i wyłącznie w sieciach o stałej strukturze. Mechanizmy koordynacji pracy stacji, niezbędne do zapewnienia periodycznego dostępu do kanału, implementowane są zazwyczaj w punktach dostępu AP do infrastruktury sieciowej. W przypadku realizacji mechanizmów koordynacji punktowej PCF w pracy kanału definiuje się tzw. superramkę czasową, w której wydziela się przedziały czasu przeznaczone na bezkolizyjną obsługę zgłoszeń synchronicznych (z ograniczeniami czasowymi) oraz rywalizacyjną obsługę zgłoszeń asynchronicznych. Przykładowa struktura superramki pokazana jest na rysunku 5.10.



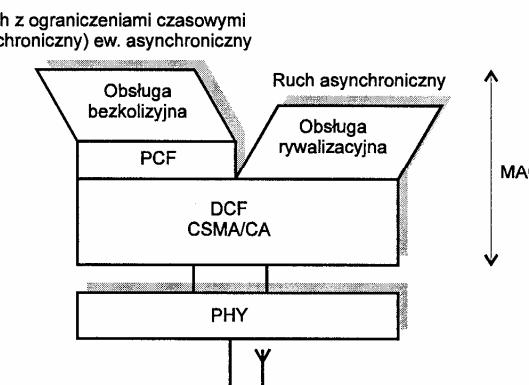
Rys. 5.10. Przykładowa struktura superramki

W ramach standardu DFWMAC warstwa MAC pełni szereg istotnych funkcji. Poza świadczeniem usług transportowych podwarstwie LLC oraz sterowania dostępem do medium, do zadań tej warstwy należą:

- koordynacja pracy stacji - szczególnie istotna w trybie PCF;
- nadzorowanie pracy stacji w celu zapewnienia przedłużonej żywotności baterijnych układów zasilających. W przypadku koncepcji z infrastrukturą sieciową i realizacją funkcji PCF stacje pozostają przez większą część czasu pracy sieci nieaktywne ("uspione"). Punkty dostępu AP buforują wówczas kierowane do nich ramki;
- monitorowanie otoczenia stacji w celu określenia pasa kanału fizycznego (w systemach wielokanałowych) oraz wyboru właściwego obszaru pracy stacji BSS (ang. *Basic Service Set*), jak też związanego z tym obszarem punktu AP;
- pełnienie funkcji kontrolnych i zarządzających pracę warstwy.

Standard DFWMAC specyfikuje kilka wersji warstwy fizycznej (w tym kanały UHF w pasmach: 1.9 GHz (podobnie jak systemy PCS), 2.4 GHz (pasmo ISM

przewidziane pierwotnie dla standardu IEEE 802.11) oraz 5.2 GHz (podobnie jak HIPERLAN), a ponadto podczerwień oraz przewiduje szybkości transmisji od 1 do 20 Mb/s. Strukturę warstwową standardu IEEE 802.11 ilustruje rysunek 5.11.



Rys. 5.11. Struktura warstwowa standardu DFWMAC

### 5.3.2 Protokół DFWMAC dla komunikacji asynchronicznej DCF

Asynchroniczny tryb pracy stanowi podstawową wersję standardu IEEE 802.11. *Transmisje asynchroniczne (tryb DCF)* realizowane są z wykorzystaniem rozbudowanego algorytmu CSMA nazywanego CSMA/CA (ang. CA - Collision Avoidance). Algorytm ten stanowi odmianę algorytmu CSMA/CD możliwą do zaimplementowania w kanale radiowym. Protokół dostępu CSMA/CA posiada w stosunku do CSMA (bądź CSMA/CD IEEE 802.3) szereg nowych elementów. Należą do nich:

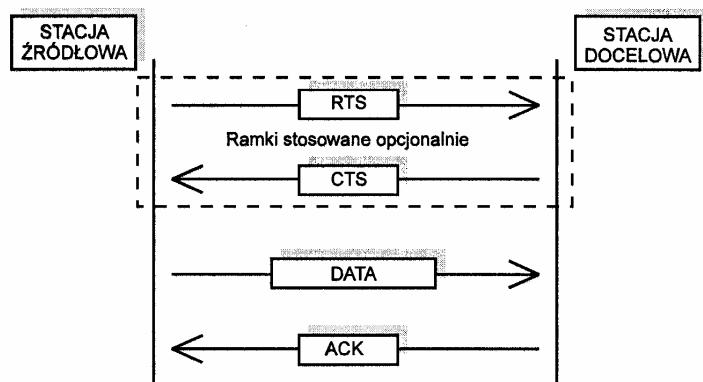
- różnicowane czasy opóźnień (w podejmowaniu różnych działań protokołarnych), dostosowane do priorytetów przesyłanych wiadomości;
- specjalne pakiety (ramki) sterujące: RTS (ang. *Request To Send*) i CTS (ang. *Clear To Send*), pozwalające na wstępную rezerwację medium i szybsze rozwiązywanie ewentualnych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

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

- istnieje potrzeba przesyłania długich pakietów DATA, bądź też
- w sieci mamy do czynienia z tzw. stacjami ukrytymi, tj. znajdującymi się poza zasięgiem bezpośredniej słyszalności stacji (sieć z transmisją wieloetapową). Istnienie stacji ukrytych (ang. *hidden stations*) w sposób istotny obniża efektywność algorytmów CSMA. Niekorzystny wpływ stacji ukrytych na jakość protokołu CSMA może być znacznie ograni-

czony poprzez zastosowanie algorytmu DCF z opcjonalnym wykorzystaniem ramek (pakietów) RTS/CTS.

W omawianym standardzie zakłada się, że wszystkie jednoadresowe ramki DATA muszą być powiadamiane pozytywnie ramkami ACK. Również ramki RTS wymagają potwierdzenia ramkami CTS. Ilustruje to rysunek 5.12.



Rys. 5.12. Przykładowa wymiana ramek między stacją źródłową i docelową

Jednocześnie w trybie DCF nie potwierdza się ramek wieloadresowych (por. też standard ETSI HIPERLAN).

Przyjęty w DFWMAC system zróżnicowanych opóźnień w podejmowaniu działań protokołarnych umożliwia obsługę zgłoszeń z różnymi priorytetami. Wyróżnia się przy tym trzy typy priorytetów:

- priorytet najwyższy - priorytet ten wykorzystywany jest do przesyłania natychmiastowych odpowiedzi zarówno w trybie DCF jak i PCF. Krótki czas reakcji stacji określany jako SIFS (ang. *Short Inter-Frame Space*) dotyczy powiadamiania ramek DATA i RTS ramkami ACK i CTS (odpowiednio), jak też reagowania stacji na przepytywanie (ang. *polling*) w trybie PCF.
- priorytet PCF - priorytet ten związany jest z czasem reakcji PIFS (ang. PCF - *Inter-Frame Space*) i odnosi się do działań podejmowanych przez punkt dostępu AP. W przypadku realizacji algorytmów PCF działania te dotyczą głównie przesyłania ramek zapytania i selekcji stacji podległych w okresie bezkolizyjnych transmisji, w trakcie superramki.
- priorytet DCF - priorytet ten, odpowiadający czasowi reakcji DIFS (ang. *DCF Inter-Frame Space*), jest wykorzystywany w przypadku realizacji algorytmu DCF. Stacje pracujące w trybie asynchronicznym monitorują

stan medium przez okres nie krótszy niż DIFS i dopiero w przypadku stwierdzenia swobody tego kanału przez okres jego monitorowania podejmują transmisje ramek DATA lub RTS.

### 5.3.2.1 Algorytm DCF

*Każda stacja chcąc uzyskać dostęp do medium musi stwierdzić swobodę kanału przez odpowiedni czas IFS (ang. *Inter-Frame Space*) przewidziany protokołem. Jeżeli w chwili nasłuchu kanał jest zajęty inną transmisją, ta stacja czeka na jej zakończenie, po czym, po czasie określonym jako DIFS (ang. *Distributed Inter-Frame Space*) przechodzi do tzw. procedury losowej retransmisji. Zadaniem tej procedury jest randomizacja prób transmisji, mająca na celu ograniczenie prawdopodobieństwa interferencji.*

Jeżeli w chwili rozpoczęcia nasłuchu kanał jest wolny, to po czasie DIFS stacja przechodzi do stanu nadawania. W przypadku stosowania mechanizmu RTS/CTS stacja poprzedza wysłanie ramki DATA krótką ramką RTS. Ramka ta - po bezbłędnym (bezinterferencyjnym) odbiorze przez stację docelową - zostaje potwierdzona ramką CTS. W przypadku ewentualnej kolizji ramek RTS, lub wcześniejszego rozpoczęcia odbioru przez stację docelową innej ramki informacyjnej DATA, ramka CTS nie zostaje przesłana.

Każda stacja nie będąca adresatem ramki RTS pozostaje po jej odbiorze nieaktywna przez czas tzw. wirtualnej zajętości kanału. Czas tej zajętości jest przy tym deklarowany przez stację źródłową w ramce RTS i retransmitowany przez stację docelową w ramce CTS. Odpowiednie czasy zajętości akceptowane przez stacje słyszące RTS i CTS określone są mianem wektorów alokacji kanału/sieci NAV (ang. *Network Allocation Vector* - NAV (RTS) i NAV (CTS)).

Zgodnie z asynchronicznym protokołem DCF wszystkie transmitowane ramki DATA muszą być powiadamiane pozytywnie ramkami ACK.

Ponadto DCF/DFWMAC przewiduje możliwość realizacji transmisji różnych typów pakietów z 2-ma priorytetami. Priorytety w transmisji realizowane są w oparciu o zróżnicowane wartości czasów IFS dostępu do medium:

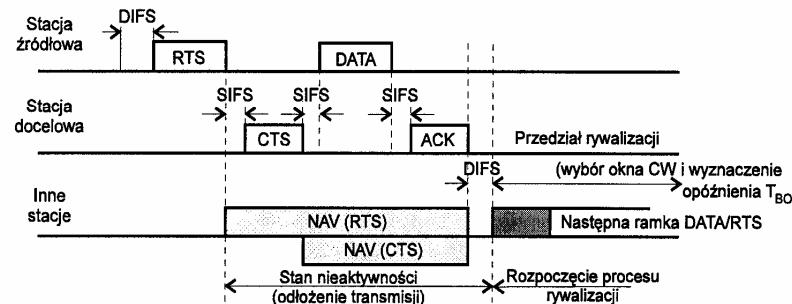
**SIFS** - czas, po którym muszą być przesłane ramki CTS bądź ACK, po uprzednim odbiorze ramek RTS bądź DATA (odpowiednio);

**DIFS** - stosowany przy transmisji ramek RTS i DATA w trybie asynchronicznym.

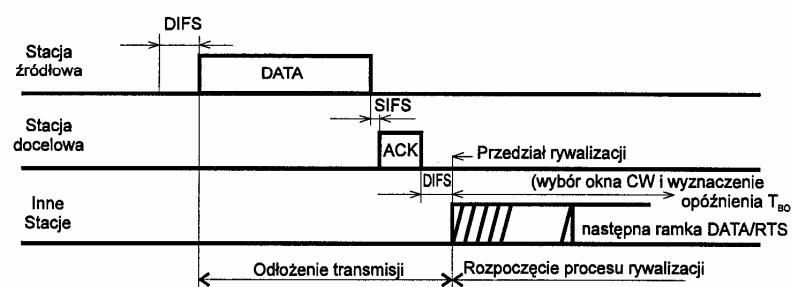
Podczas pracy stacje aktywne (realizujące wymianę informacji) uaktualniają kilka zegarów. Przykładowo zegar T1 odmierza czas upływający od nadania RTS. Jeżeli w czasie T1 - przewidzianym protokołem - zostanie odebrana ramka CTS, wówczas po czasie SIFS zostaje wysłana ramka DATA.

W przeciwnym przypadku stacja przechodzi w tryb losowej retransmisji. Podobna procedura jest wdrażana, gdy po nadaniu ramki DATA powiadomienie ACK nie zostanie odebrane przez czas T3.

W trybie retransmisji stacja, po odczekaniu okresu DIFS, generuje losowy przedział czasu, po którym ponawia próbę dostępu. Czas ten jest wielokrotnością czasu trwania tzw. szczelin czasowej - wielkości będącej parametrem systemowym. Działanie algorytmu DCF/DFWMAC z wykorzystaniem, bądź nie, mechanizmu RTC/CTS ilustrują rysunki 5.13 i 5.14.



Rys. 5.13. Ilustracja algorytmu DCF z mechanizmem RTS/CTS



Rys. 5.14. Ilustracja realizacji algorytmu DCF z pominięciem ramek RTS/CTS

Należy zwrócić uwagę na możliwość wystąpienia zarówno pozytywnych jak i negatywnych aspektów stosowania mechanizmu RTS/CTS. Wybitnie korzystny wpływ pakietów RTS/CTS na efektywność pracy sieci LAN obserwujemy w przypadku transmisji długich pakietów DATA. Efekty negatywne można natomiast zaobserwować, gdy przesyłane są głównie krótkie pakiety DATA. Algorytm DCF ma wbudowane procedury pozwalające na porównywanie długości ramek DATA, gotowych do transmisji, z wartością progową przyjętą dla danego systemu RLAN, po przekroczeniu której ramki RTS/CTS winny być stosowane.

Algorytm DCF umożliwia też przesyłanie przez jedną stację serii ramek, bez konieczności każdorazowej rywalizacji o prawo dostępu. Kolejne ramki i powiadomienia ACK przesyłane są z odstępem SIFS.

W literaturze proponowane są i rozważane również inne algorytmy pracy bezprzewodowych sieci LAN, w tym odmienne od prezentowanego protokoły MAC typu CSMA/CA, pozwalające bądź na wcześniejsze wykrywanie kolizji, bądź też znaczne ograniczenie wpływu kolizji długich pakietów DATA.

### 5.3.2.2 Algorytm rywalizacji o dostęp do medium i realizacji retransmisji ramek (ang. Access Backoff Procedure)

W przypadku, gdy stacja chcącą uzyskać dostęp do kanału stwierdza jego zajętość, wówczas odkłada próbę dostępu do chwili wykrycia przerwy (braku aktywności w kanale) o długości DIFS. Gdy odliczany przez stację czas przerwy w pracy kanału przekracza wartość DIFS, stacja generuje losowy czas opóźnienia dostępu (ang. random backoff period). Procedura randomizacji dostępu pozwala w znacznym stopniu wyeliminować kolizje ramek. Wartość losowego czasu opóźnienia  $T_{BO}$  (ang. Backoff) w dostępie stacji określa zależność:

$$T_{BO} = CW * \text{Random0} * \text{Długość szczeliny}$$

gdzie

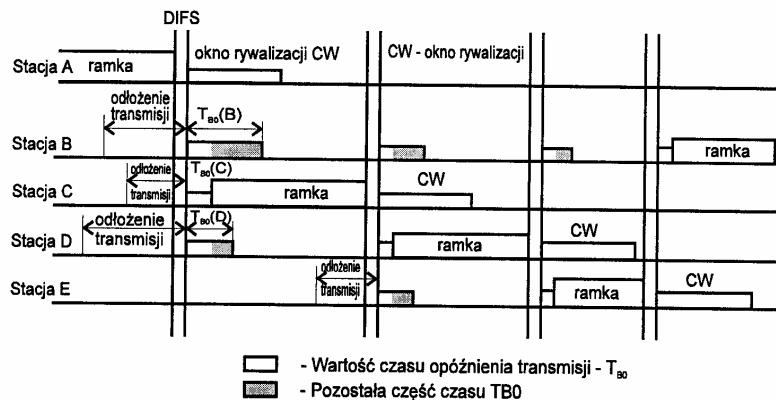
$CW$  - szerokość okna rywalizacji (czyli maksymalna wartość opóźnienia w danej próbie dostępu do medium, wyrażona liczbą szczelin czasowych).

Długość szczeliny - czas obejmujący maksymalne opóźnienie propagacyjne w medium oraz czasy przełączania nadajnika i podejmowania decyzji o zajętości kanału. Czas trwania szczeliny jest zależny od typu medium i rozwiązania warstwy fizycznej.

Random0 - reprezentuje wartość losową z przedziału  $<0, 1>$ .

W przypadku realizacji procedury randomizacji dostępu, początkowa wartość szerokości okna CW ustawiana jest jako  $CW_{min}$ . Po każdej nieudanej transmisji wartość CW jest podwajana (podobnie jak w IEEE 802.3). Ma to na celu zapewnienie stabilnej pracy sieci przy dużym jej obciążeniu. Niediana próba transmisji to próba kończąca się interferencją. Oznacza to, że liczniki czasu  $T_{BO}$  odliczające chwilę dostępu do medium wyzerowały się w dwóch lub więcej stacjach w tej samej szczelinie.

W sytuacji, gdy początkowe stany liczników  $T_{BO}$  stacji rywalizujących o dostęp są różne, wówczas tylko jedna spośród nich rozpocznie bezinterferencyjnie swoją transmisję - po wyzerowaniu się jej licznika. Pozostałe stacje zatrzymują swoje liczniki (zamrażają ich stany) i odkładają próbę transmisji do chwili wykrycia kolejnej przerwy DIFS. Z tą chwilą uruchamiają ponownie swoje liczniki  $T_{BO}$  (bez dokonywania losowania nowej wartości  $T_{BO}$ ). Pierwszy z zerujących się liczników wskazuje na prawo dostępu danej stacji do medium. Tym samym, o ile nie następuje interferencja ramki, opóźnienie w czasie dostępu do medium systematycznie maleje. Ilustruje to rysunek 5.15.



Rys. 5.15. Ilustracja algorytmu rywalizacji

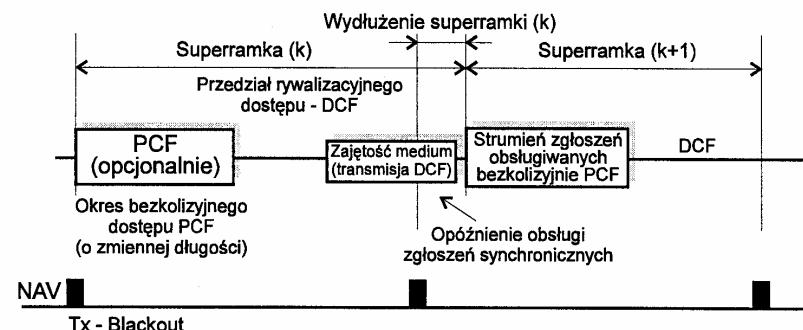
### 5.3.3 Protokół PCF dla obsługi ruchu synchronicznego

*Protokół DFWMAC realizuje opcjonalnie tzw. punktową funkcję koordynacji dostępu PCF zapewniającą bezkolizyjny przekaz danych. Odpowiada to realizacji usług połączeniowych. Opcja PCF może być zaimplementowana jedynie w sieci RLAN ze stałą infrastrukturą, w szczególności z wydzielonym jednym lub wieloma punktami dostępu AP.* Podstawowym warunkiem realizacji protokołu PCF jest brak wzajemnego oddziaływanie obszarów pracy sieci (ang. BSA - Basic System Area) skupiających stacje BSS (ang. Basic System Set) korzystające z różnych punktów AP. Niespełnienie tego wymogu może prowadzić do kolizji pomiędzy stacjami należącymi do różnych grup BSS, korzystających z tego samego kanału. Kolizje te nie mogłyby być rozwiązyane przez procedury PCF. Z powyższego sformułowania wynika, że w przypadku pokrywania się obszarów BSA, stacje w każdym z nich muszą korzystać z odrębnych kanałów, zapewniających tym samym wzajemną separację poszczególnych segmentów sieci.

W przypadku realizacji protokołu PCF, standard DFWMAC oferuje usługi zarówno asynchroniczne, jak też z ograniczeniami czasowymi. Podział czasu pomiędzy dwa typy usług dokonywany jest przez stację AP zarządzającą tzw. superramką czasową. W protokole PCF definiowana jest superramka o postaci pokazanej na rysunku 5.16. W ramach superramki algorytmy PCF są odpowiedzialne za dostęp stacji do medium w okresie bezkolizyjnych transmisji. Z kolei druga część ramki wykorzystywana jest w trybie rywalizacyjnym (kolizyjnym) dostępu, zgodnie z procedurą DCF.

Okres bezkolizyjnego dostępu CFP (ang. Contention Free Period) może mieć losową długość o znacznych wahaniach. Z kolei długość całej superramki ulega jedynie nieznacznym zmianom. Każdorazowo, w momencie początkowym super-

ramki, algorytm PCF stacji zarządzającej dostępem (zwykle AP) przejmuje pełne sterowanie dostępem do medium. Algorytm PCF nie wymusza jednakże wcześniejszego zakończenia transmisji ramki DATA obsługiwanej zgodnie z DCF. Z chwilą rozpoczęcia się superramki, inicjowanej przez PCF, po stwierdzeniu przerwy w transmisji w kanale o długości PIFS, wszystkie transmisje ramek asynchronicznych zostają odłożone do chwili rozpoczęcia się okresu rywalizacji CP (ang. Contention Period). Rozpoczęcie kolejnej superramki wiąże się z generacją w stacji AP specjalnego sygnału TX-Blackout. Jeżeli jednakże w chwili generacji tego sygnału w kanale jest prowadzona transmisja asynchroniczna, to stacja AP opóźnia rozpoczęcie okresu CFP do chwili zakończenia tej transmisji.



Rys. 5.16. Ilustracja organizacji superramki w przypadku realizacji protokołu PCF

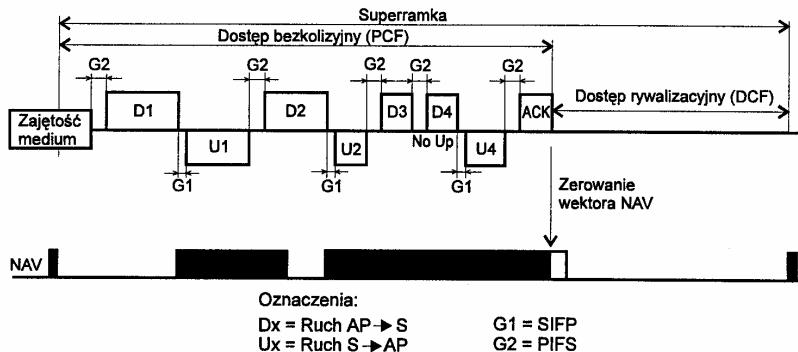
Długość superramki może ulegać zmianie, zgodnie ze zgłaszanymi żądaniami usług połączeniowych. Jest też ona parametrem uzależnionym od rozwiązania warstwy fizycznej.

### Protokół wymiany informacji między stacją AP a stacjami podległymi

*Protokół dostępu PCF oparty jest na metodzie przepływu.* Stacje chcąc uzyskać usługę typu synchronicznego muszą zgłosić stosowne żądania do AP. W przypadku akceptacji tych żądań, stacje zostają włączone przez AP na listę stacji przepływywanych (ang. Polling List - PL). Proces rezerwacji dostępu do medium realizowany jest za pośrednictwem ramek asynchronicznych, przesyłanych w trybie DCF. Tym samym mechanizm DCF wykorzystywany jest do zestawienia połączenia pomiędzy obiektami MAC, obsługiwany następnie w trybie synchronicznym (z ograniczeniami czasowymi). Przykład realizacji mechanizmu przepływu zgodnie z procedurą PCF ilustruje rysunek 5.17.

AP przesyła w okresie CFP do stacji końcowych między innymi ramki, które były uprzednio buforowane przez tę stację AP. Specjalny bit w nagłówkach ramek

kierowanych do stacji podległych (końcowych) zaprasza te stacje do przesyłania ich własnych ramek. Reakcje stacji są natychmiastowe, zgodnie z najwyższym priorytetem - odpowiadającym opóźnieniu SIFS.

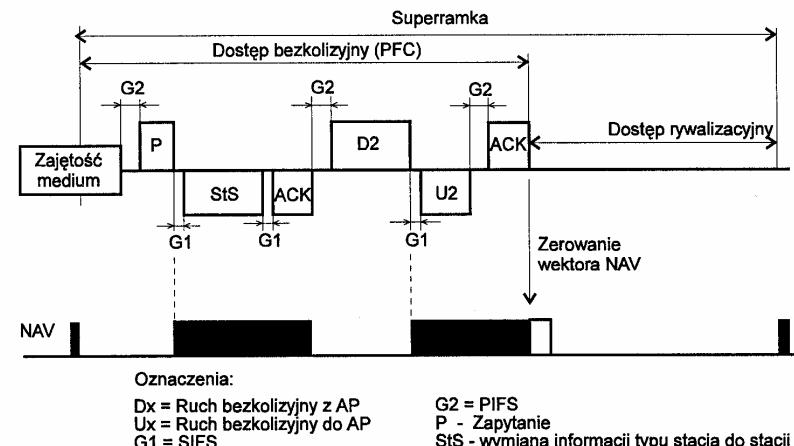


Rys. 5.17. Realizacja procesu przepływu stacji zgodnie z procedurą PCF

Powiadomienia ACK przesyłane w obu kierunkach mogą być dołączane do ramek DATA, bądź też przesyłane jako niezależne. Długości ramek DATA mogą być dowolne, ograniczone jedynie maksymalną wartością negocjonowaną w fazie zgłoszenia żądania obsługi. Brak reakcji stacji na zaproszenie do nadawania w okresie SIFS powoduje ponowne przejęcie kontroli nad medium przez AP i skierowanie zapytania do kolejnej stacji z listy PL. W nagłówkach ramek przesyłanych przez AP dokonywana jest każdorazowo modyfikacja parametrów wektora NAV zajętości kanału. Zmodyfikowana wartość wektora NAV jest następnie retransmitowana przez stacje podległe. W chwili wyczerpania listy PL (zakończenia okresu przepływu) stacji obsługiwanych w trybie synchronicznym, stacja AP przesyła ramkę ACK lub BEACON z wyzerowaną wartością wektora NAV. Stanowi to informację o zakończeniu okresu CFP i rozpoczęciu rywalizacji o dostęp do kanału po czasie DIFS.

#### Wymiana ramek między stacjami danego obszaru

Algorytm PCF pozwala również sterować przepływem ramek między stacjami podległymi danego obszaru BSA. W tym przypadku AP jedynie inicjuje proces przekazu, przesyłając ramkę typu POLL (zapytanie) do pierwszej stacji z listy PL. Stacja zaproszona do nadawania przesyła ramkę DATA po czasie SIFS. Jeżeli ramka DATA zawiera adres podległej stacji docelowej, wówczas stacja ta po czasie SIFS przekazuje powiadomienie ACK. Brak aktywności w kanale przez czas PIFS powoduje ponowne przejęcie kontroli nad pracą sieci przez stację AP. Przykładowy przebieg wymiany informacji zgodnie z powyższymi zasadami ilustruje rysunek 5.18.



Rys. 5.18. Realizacja mechanizmu bez przepływu z elementami przekazywania TOKENa; Protokoł PFC z możliwością wymiany informacji między stacjami ruchomymi

#### Typy usług realizowanych w trybie bezkolizyjnym

*Procedury PCF pozwalają na realizację zarówno usług synchronicznych (z ograniczeniami czasowymi) jak i asynchronicznych.* W obu przypadkach wykorzystywany jest ten sam algorytm PCF. Odmienne są jednakże zasady rezerwacji, mechanizmy adresacji i formaty ramek. PCF stosuje też różne mechanizmy alokacji czasu obsługi dwóch powyższych typów ramek. Okres bezkolizyjny CFP musi być ograniczony by zapewnić możliwości obsługi ruchu asynchronicznego. Minimalna długość okresu rywalizacji CP w ramach superramki nie może być przy tym mniejsza od najdłuższej ramki przesyłanej w trybie asynchronicznym DCF.

$$t(CFP) = t(\text{superramki}) - t(\text{max długość ramki asynchronicznej})$$

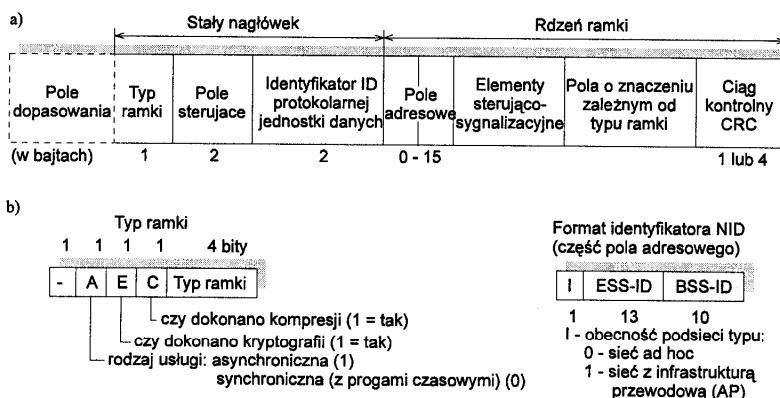
Pozwala to na obsługę przynajmniej jednej ramki asynchronicznej w każdym cyklu obsługi.

#### 5.3.4 Struktury ramek w IEEE 802.11

Podstawową jednostką informacji przesyłaną między obiektami MAC jest rama. Pełna protokolarna jednostka danych podwarstwy MAC, tzw. jednostka MPDU może jednakże w standardzie IEEE 802.11 składać się z ciągu ramek (np. RTS - CTS - DATA - ACK lub DATA - ACK) wymienianych pomiędzy dwoma obiektami. W takim przypadku wzajemne zależności pomiędzy kolejnymi ramkami są podawane w ich nagłówkach - w postaci identyfikatorów MPDU-ID.

Każda ramka składa się z kilku podstawowych pól. Należą do nich:

- **nagłówek dopasowujący ramkę do wymagań warstwy fizycznej** - o stałej długości i o postaci zależnej od rodzaju medium fizycznego (ang. *PHY Adaptation Header*);
- **stalą długości nagłówek podwarstwy MAC** zawierający:
  - pole typu ramki (ang. *type field*),
  - pole sterujące (ang. *control field*),
  - identyfikator ID protokolarnej jednostki danych MPDU.
- **rdzeń ramki** (ang. *frame body*) obejmujący:
  - pola adresowe, które mogą zawierać jeden lub więcej segmentów z identyfikatorem NID sieci (ang. *Network ID*), adresem docelowym i/lub źródłowym (w zależności od typu ramki),
  - zmiennej długości elementy sterująco-sygnalizacyjne (ang. *elements*) i pola o znaczeniu zależnym od typu ramki (ang. *type-dependent fields*),
  - dane sterujące - pole o zmiennej długości - zawierające informacje z podwarstwy LLC (w przypadku ramek DATA).
- **ciąg kontrolny CRC** - 8-mio lub 32-bitowy w zależności od typu ramki.



Rys. 5.19. Ilustracja struktury ramki w standardzie IEEE 802.11: a) pełna ramka, b) znaczenie bitów pól typu ramki i pól adresu

Postać ramki i znaczenie poszczególnych pól prezentuje rysunek 5.19. Pierwsze jednobajtowe pole nagłówka ramki MAC (pole typu ramki) zawiera między innymi 4 bity definiujące typ ramki i 3 bity zarządzające. Bity zarządzające wskazują na rodzaj realizowanej usługi (asynchroniczna, synchroniczna), stosowanie,

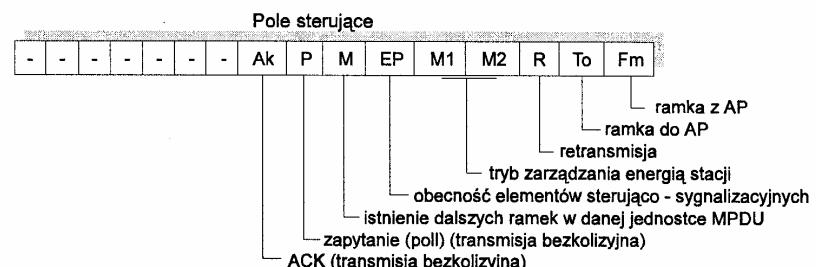
lub nie, zabezpieczeń kryptograficznych oraz dokonanie, bądź nie, kompresji ramki. W przypadku usługi asynchronicznej standard 802.11 definiuje następujące ramki:

1. RTS
2. CTS
3. DATA
4. ACK
5. POLL (ramka zapytania)
6. BEACON (ramka sygnalizacyjna)
7. ATIM (ramka z informacją o danych buforowanych w AP)
8. REQUEST (ramka żądania)
9. RESPONSE (ramka odpowiedzi)

W przypadku realizacji usługi synchronicznej (z ograniczeniami czasowymi) mamy z kolei następujące rodzaje ramek:

1. TB-Up (ramki ze stacji podległej do stacji AP)
2. TB-Down (ramki ze stacji AP do stacji podległej)
3. TB-CTS (ramki AP zapraszające stacje końcowe do retransmisji)
4. ACK

Pole sterujące w ramce jest dwubajtowe. Znaczenie poszczególnych bitów tego pola wyjaśnia rysunek 5.20.



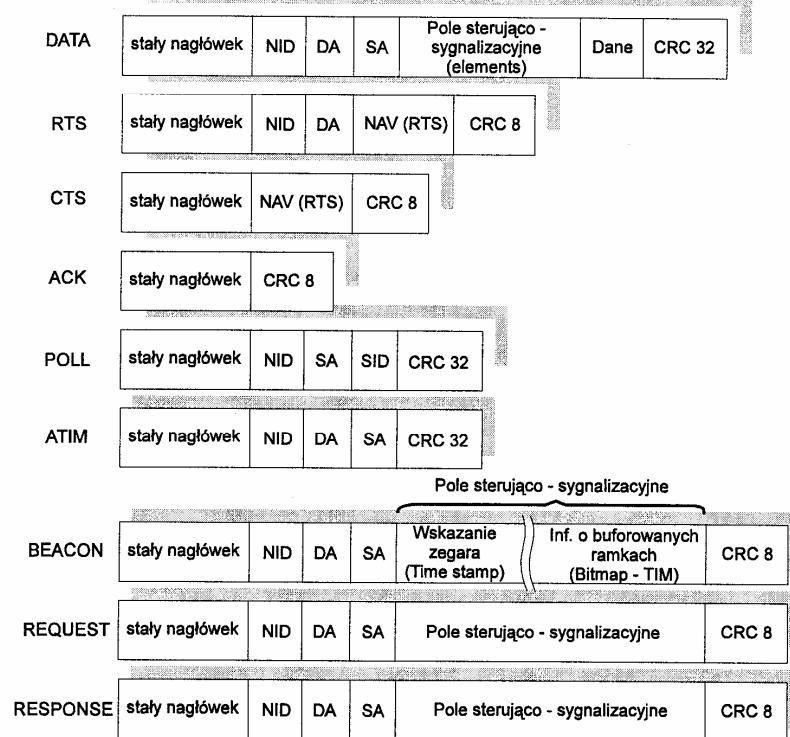
Rys. 5.20. Znaczenie bitów pola sterującego ramki standardu 802.11

Kolejne 16-sto bitowe pole zawiera bądź wartość identyfikatora ID protokolarnej jednostki danych MPDU - w przypadku ramek asynchronicznych, bądź też wartość identyfikatora połączenia (connection ID) - w przypadku ramek synchronicznych.

W polu adresowym ramki może znajdować się identyfikator NID sieci i/lub 48-mio bitowe indywidualne lub grupowe adresy stacji (adres źródłowy lub docelowy, żaden z nich lub oba - w zależności od typu ramki) - zgodnie ze standardem IEEE.

3 bajtowy identyfikator sieci NID obejmuje bity rodzaju sieci (sieć rozproszona, typu ad-hoc, bądź sieć ze stałą infrastrukturą) oraz identyfikatory obszarów: podstawowego BSA (10-bitowy BSS-ID) i rozszerzonego ESS (13-bitowy ESS-ID).

#### Typy ramek:



Rys. 5.21. Przykładowe postacie ramek informacyjnych i sterujących

W zależności od typu ramki jej "rdzeń" może ulegać istotnym zmianom. Przykłady ramek informacyjnych i sterujących przepływem informacji między obiektami MAC ilustruje rysunek 5.21. Występujące w różnych typach ramek pola sterująco-sygnalizacyjne (tzw. elements) zawierają ważne informacje (parametry) zarządzająco-kontrolne. Obejmują one między innymi wartości wskazań zegarów stacji, wartości przedziałów czasu pomiędzy kolejnymi ramkami sygnalizacyjnymi typu BEACON, informacje o ramkach buforowanych w stacjach AP, czy też odstępy czasu pomiędzy tzw. nienegociowanymi retransmisjami ramek buforowanych w punktach dostępu AP.

Zgodnie z ilustracją z rysunku 5.21 stosunkowo krótkie ramki sterujące typu RTS, CTS i ACK są zabezpieczone kodem cyklicznym generowanym przez wielomian stopnia ósmego, podczas gdy pozostałe ramki, w tym ramki DATA, są zabezpieczone 32-pozycyjnymi ciągami kodu cyklicznego.

Przyjmuje się, że długości ramek nie przekraczają 1500 bajtów (podobnie jak w standardzie IEEE 802.3).

#### 5.3.5 Jakość oferowanych usług

W standardzie IEEE 802.11 *wysoka jakość oferowanych usług, zarówno połączeniowych jak i bezpołączeniowych, gwarantuje realizacja mechanizmów wykrywania nieprawidłowości w pracy sieci*. Podstawowym elementem tych mechanizmów jest zasada potwierdzania ramek. W przypadku obsługi ramek z ograniczeniami czasowymi, czyli realizacji protokołu PCF, pojawienie się jakiegokolwiek błędu w ramce typu TB-Down (ramki z AP do stacji końcowych) lub TB-Up (ramki ze stacji końcowych do AP) zostaje wykryte w okresie TBFP (ang. *Time Bounded Frame Period*) stanowiącym wielokrotność czasu trwania superramek. Retransmisja zniększałonej lub zagubionej ramki musi nastąpić przed generacją kolejnej (nowej) ramki w danym połączeniu. Protokół PCF może w celu obsługi dodatkowych - retransmitowanych ramek rozszerzyć przedział bezkolizyjnej transmisji w obrębie superramki. W przypadku błędnej ramki typu TB-Down stacja AP dokonuje jej retransmisji. Z kolei w przypadku błędu w ramce ze stacji końcowej, stacja AP przesyła ramkę TB-CBS zapraszając stację końcową do retransmisji jej ramki (TB-Up).

#### Przykładowe procedury utrzymywane sieci

W przypadku radiowych sieci teleinformatycznych, w których stacje końcowe korzystają prawie wyłącznie z zasilania baterijnego, problem efektywnego użytkowania energii nabiera szczególnego znaczenia. Warstwa MAC winna realizować procedury dostępu tak, by oszczędnie gospodarować zasobami energetycznymi stacji. W zakresie wydatkowania energii standard 802.11 definiuje 4 tryby pracy stacji:

1. tryb aktywności ciągłej CAM (ang. *Continuous - Active Mode*), w którym stacja może nadawać i odbierać ramki w dowolnym czasie; żadne ramki nie są też buforowane przez AP, tryb CAM jest właściwy jedynie dla stacji z zasilaniem stałym;
2. tryb okresowej aktywności - TAM (ang. *Temporary - Active Mode*), w którym stacja okresowo przechodzi do stanu aktywnego;
3. tryb oszczędnej pracy bez powiadamiania o retransmisji ramek buforowanych przez AP - PSNV (ang. *Power-Save Non-Polling*), w którym stacja włącza się jedynie w okresach transmisji informacji DTIM o ramkach buforowanych w AP i retransmitowanych przez AP bez zapytania stacji (sprawdzenie jej gotowości) do ich odbioru (ramką POLL); tryb bez "negocjacji" retransmisji ramek buforowanych;

4. tryb oszczędnej pracy z zapraszaniem do odbioru (z negocjacją odbioru) ramek buforowanych przez AP - PSP (ang. *Power-Save-Polling*), w którym stacja włącza się (przechodzi w stan aktywny) w okresach przesyłania informacji TIM o ramkach buforowanych przez AP. W tym przypadku buforowane ramki są retransmitowane do stacji końcowych jedynie po pozytywnej odpowiedzi stacji na zaproszenie typu POLL.

Wymienione powyżej informacje sterujące TIM (ang. *Traffic Indication Map*) oraz DTIM (ang. *Delivery TIM*) przesyłane są głównie w ramkach sygnalizacyjnych typu BEACON. Ramki BEACON pełnią kilka ważnych funkcji. Służą one do synchronizacji pracy stacji, zarówno w sieci o strukturze ad-hoc jak i w sieciach z infrastrukturą stałą. Pozwalają tym samym na pracę stacji w trybach oszczędnych. Informacja zawarta w ramkach typu BEACON (TIM/DTIM) umożliwia też identyfikację (w przypadku realizacji protokołu PCF) ramek buforowanych w stacjach AP i adresowanych do stacji końcowych. W przypadku stwierdzenia przez stację końcową obecności w AP pakietów przeznaczonych dla danej stacji, przechodzi ona na czas ich odbioru w stan aktywny. Ramki BEACON zawierają też identyfikatory NID generujących je stacji (w szczególności stacji AP w przypadku realizacji PCF). Pozwalają one tym samym na pasywne monitorowanie sieci przez stacje chcącą dołączyć się do sieci RLAN. NID zawiera bowiem niezbędne identyfikatory danego obszaru sieci. Przyjmuje się, że ramki sygnalizacyjne typu BEACON przesyłane są periodycznie co 20 - 50 milisekund. Innym typem ramki utrzymywanej jest ramka próbna (PROBE) służąca do testowania (monitorowania) stanu sieci. Ramka typu PROBE pozwala zarówno na synchronizację sieci, jak też ustalenie zbioru stacji słyszących się wzajemnie na obszarze BSS. Ramka PROBE wykorzystywana jest również do aktywnego monitorowania otoczenia stacji w celu jej włączenia się do sieci lub też zmiany obszaru działania stacji. Po wysłaniu ramki PROBE stacja przechodzi w stan nasłuchu. Czas monitorowania kanału jest rzędu 2 milisekund. W przypadku braku reakcji ze strony stacji dokonywane jest badanie kolejnych kanałów przydzielanych do transmisji dla sieci RLAN.

#### 5.4 Standard ETSI - HIPERLAN dla radiowych sieci LAN

W najbliższych latach bezprzewodowe sieci komputerowe będą stanowiły przedmiot znacznego zainteresowania zarówno producentów jak i użytkowników tego typu instalacji. Będą one też odgrywać istotną rolę w rozległych strukturach sieciowych zapewniając dostęp do przewodowej infrastruktury sieci LAN, MAN i WAN. Przewiduje się, że łatwy dostęp do sieci będą posiadały zarówno popularne "laptopy" - o stosunkowo dużej mocy obliczeniowej - jak też proste urządzenia wielkości obecnych aparatów przywoławczych.

W celu efektywnego rozwiązania łączności o wymaganej jakości transmisji i szybkości rzędu kilku do kilkudziesięciu Mb/s, nieodzowne jest opracowanie

standardowych styków pomiędzy elementami złożonej architektury sieciowej. Zagadnienia te stanowią przedmiot prac Europejskiego Instytutu Standardów Telekomunikacyjnych ETSI (ang. *European Telecommunications Standards Institute*). ETSI opracowuje standardowe rozwiązanie protokolarne dla bezprzewodowej sieci LAN nazywane HIPERLAN (ang. *HIGH PErformance Radio LAN*). Prace ETSI koncentrują się głównie na zdefiniowaniu usług oraz specyfikacji protokołów realizujących funkcje podwarstw: dostępu do medium MAC oraz sterowania dostępem do kanału CAC (ang. *Channel Access Control Sublayer*) - tworzących dwie dolne podwarstwy WŁD. Standard ETSI obejmuje też w pełni problemy funkcjonowania warstwy fizycznej (WF), łącznic z zagadnieniami przydziału pasm częstotliwości, systemów antenowych, synchronizacji transmisji, modulacji, kodowania, mocy sygnałów, itp.

Sieć HIPERLAN jest podsystemem komunikacji radiowej pozwalającym na realizację transmisji o niewielkim zasięgu (do kilkuset metrów) z dużymi szybkościami. Ramki tworzone w podwarstwie CAC są przy tym przesyłane z dwiema szybkościami:

- z małą szybkością (ang. *Low Bit Rate*) równą  $1.4706 \text{ Mb/s} \pm 15 \text{ b/s}$   
w tzw. części LBR ramek oraz
- z dużą szybkością (ang. *High Bit Rate*) równą  $23.5294 \text{ Mb/s} \pm 235 \text{ b/s}$   
- w tzw. części HBR ramek.

Transmisje realizowane są w paśmie od 5.15 GHz do 5.30 GHz. W paśmie tym wydzielanych jest 5 podkanałów (częstotliwości nośnych odległych o około 23.5 MHz). Sygnały w części LBR ramek modulowane są z wykorzystaniem FSK. Z kolei metoda GMSK (ang. *Gaussian Minimum Shift Keying*) jest stosowana do modulacji ciągu danych w części HBR ramek. Zwrócić uwagę, że modulacja GMSK jest też stosowana w systemie radiotelefonii komórkowej GSM.

Do wykorzystania w sieci HIPERLAN przewidywane jest też pasmo częstotliwości 17.1 GHz do 17.3 GHz.

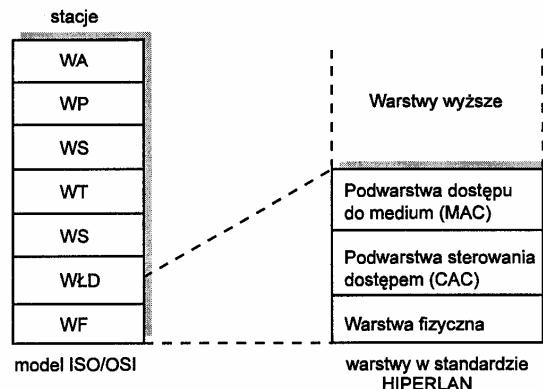
##### 5.4.1 Podstawowe funkcje i usługi oferowane przez HIPERLAN

Architektura standardu HIPERLAN obejmuje podwarstwy MAC i CAC oraz warstwę fizyczną. Strukturę warstwową standardu ilustruje rysunek 5.22.

Zgodnie z podstawowymi założeniami HIPERLAN powinien zapewniać współpracę ze standardowymi rozwiązaniami IEEE 802.2 (ISO 8802.2). Podstawowe cechy systemu HIPERLAN są przy tym następujące:

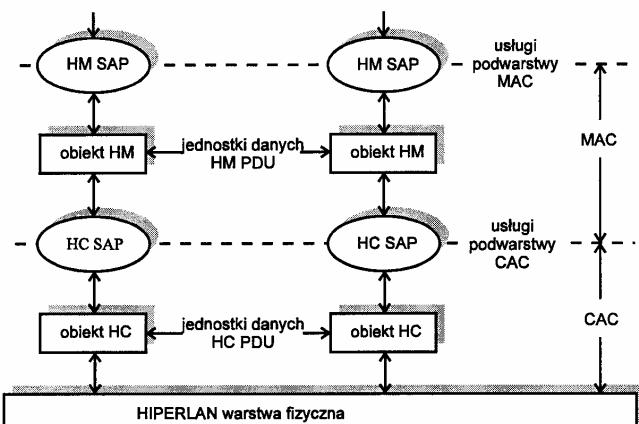
- HIPERLAN jest radiową siecią LAN (RLAN), która świadczy usługi równoważne usługom definiowanym w zaleceniach ISO dla podwarstwy MAC (ISO 15802-1);
- HIPERLAN zapewnia realizację funkcji przypisywanych mostom, zgodnie ze stosowną specyfikacją ISO, pozwalając tym samym na współpracę z innymi sieciami LAN i realizację transmisji wieloetapowych w ramach pojedynczej sieci RLAN;

- HIPERLAN zapewnia komunikację między stacjami przenośnymi i ruchomymi z wykorzystaniem wspólnego medium transmisyjnego;
- Sieć pozwala na obsługę zarówno zgłoszeń asynchronicznych, jak też ruchu z ograniczeniami narzuconymi na czas dostępu do kanału. HIPERLAN korzysta przy tym z priorytetowych mechanizmów sterowania dostępem, zapewniających "hierarchiczną" (tj. zgodną z przyjętymi priorytetami) niezależność jakości obsługi różnych strumieni zgłoszeń.



Rys. 5.22. Porównanie architektury sieci HIPERLAN i modelu ISO/OSI

Współpraca międzywarstwowa oraz komunikacja między obiektymi poszczególnych warstw odbywa się na ogólnych zasadach przyjętych w modelu ISO/OSI. Model współpracy podwarstw MAC i CAC pokazany jest na rysunku 5.23.



Rys. 5.23. Model współpracy podwarstw MAC i CAC

Pomiędzy podwarstwami LLC (użytkownik usług MAC) i MAC oraz MAC i CAC definiowane są punkty dostępu do usług, oznaczane odpowiednio HM-SAP oraz HC-SAP, tworzące logiczne interfejsy dostępu do usług świadczonych przez poszczególne podwarstwy. Dostęp do usług odbywa się za pośrednictwem zbiorów prymitywów (operacji podstawowych). W przypadku systemu HIPERLAN mamy do czynienia z odmiennymi - w stosunku do omawianych wcześniej dla sieci IEEE 802 LAN - funkcjami, usługami i zbiorami prymitywów. Usługi oferowane przez podwarstwę MAC dotyczą w szczególności:

- przekazu danych z czasowymi ograniczeniami na jego realizację, narzuconymi przez użytkownika usługi oraz
- aktywnego badania dostępności różnych stacji i sieci HIPERLAN pracujących na danym obszarze.

Protokół HIPERLAN MAC zapewnia każdej ze stacji sieci realizację stosowanych usług oraz wypełnianie przez stację funkcji mostu - zgodnie ze stosowną specyfikacją ISO. Protokół ten określa też zasady komunikacji obiektów MAC w środowisku radiowym, w tym transmisji wieloetapowych oraz typy wymienianych jednostek danych.

Przy wymianie jednostek danych podwarstwa MAC korzysta z usług podwarstwy CAC. Podwarstwa CAC sterowania dostępem zapewnia między innymi:

- hierarchiczny i niezależny dostęp do usług CAC, zgodnie z wymaganiami (parametrami) zdefiniowanymi przez obiekt (protokół) MAC;
- specyfikację priorytetowego algorytmu bez wymuszania dostępu NPMA (ang. Non-pre-emptive Priority Multiple Access)
- definicje typów ramek przesyłanych między obiektami CAC.

Ażeby zapewnić kompatybilność standardu HIPERLAN z rozwiązaniami ISO (w szczególności ISO MAC) adresy punktów dostępu HM SAP oraz HC SAP są 48-mio bitowe i odpowiadają adresom fizycznym stacji (kart sieciowych). Wyróżnia się przy tym adresy indywidualne i grupowe. Adresy HM SAP i HC SAP w danej stacji są identyczne.

Z uwagi na nieograniczoną przestrzenną kanału radiowego może dojść do wzajemnego pokrywania się obszarów działania dwóch lub większej liczby sieci HIPERLAN. W sieciach tych stosuje się więc dodatkowe identyfikatory składające się z ciągów znaków i symboli binarnych. Nie prowadzi się przy tym globalnej administracji tych identyfikatorów.

Podwarstwa MAC oferują, przy przekazie danych, usługi bezpołączeniowe. Dostęp do usług oferowanych przez podwarstwę MAC odbywa się za pośrednictwem zespołu prymitywów. Do przekazu danych wykorzystywane są:

HM - UNIDATA.request i

HM - UNIDATA.indication.

Prymitywy te jako parametry zawierają:

- adresy: źródłowy i docelowy,
- priorytet obsługi jednostki danych,
- jednostkę danych (MSDU),
- czas życia jednostki danych (ang. *lifetime*).

W sieci HIPERLAN, przy kolejnych retransmisjach ramek (jednostek danych), wyznacza się "pozostały" czas ich "życia" (ang. *residual lifetime*).

Z kolei do celów sterowania pracą sieci stosowane są prymitywy:

- HM - QOSFAILURE.indication oraz
- HM - LOOKUP.request
- i HM - LOOKUP.confirm.

Pierwszy z prymitywów (QoSFailure) umożliwia przekazanie informacji o nieudanym transferze danych na skutek upływu czasu życia jednostki danych (jest reakcją na HM - UNIDATA.request).

Kolejne prymitywy (lookup) dotyczą usługi związanej z badaniem stanu sieci HIPERLAN wokół danej stacji. W oparciu o informacje sterujące możliwa jest realizacja procedur routingu, nieodzownych przy wypełnianiu funkcji mostu.

Obiekty HM (MAC) tworzą specjalne bazy danych RIB (ang. *Routing Information Base*), które są dynamicznie uaktualniane. W przypadku braku pełnej informacji o strukturze sieci możliwe jest wysłanie jednostki danych w postaci rozgłoszeniowej (*broadcast*). Badanie stanu sieci odbywa się za pośrednictwem specjalnych jednostek danych: H (ang. *Hello*) i TC (ang. *Topology Control*); H-HMPDU i TC-HMPDU; wysyłanych przez obiekty MAC.

Standard HIPERLAN definiuje szereg typów i struktur jednostek danych HMPDU. Usługa oferowana przez podwarstwę CAC jest również usługą bezpośrednio-wiązącą. Przekaz danych pomiędzy obiektami MAC, a CAC odbywa się za pośrednictwem prymitywów:

- HC-UNIDATA.request
- HC-UNIDATA.indication.

Właściwe sterowanie wymianą informacji między obiektami związane jest z przesyaniem prymitywów typu:

- HC-SYNC.indication - z informacją o początku cyklu transmisyjnego w pracy kanału,
- HC-FREE.indication - zawierającego zgodę na obsługę kolejnej ramki oraz
- HC-STATUS.indication - potwierdzającego udaną transmisję poprzedniej jednostki danych.

Protokół CAC pozwala na przyjęcie do obsługi jednostki danych - z obiektem MAC - o maksymalnej długości 2422 bajtów.

#### 5.4.2 Typy ramek definiowanych przez protokół HIPERLAN CAC

Ograniczymy się tutaj do zaprezentowania typów i struktur ramek przesyłanych między obiektami warstwy CAC (obiekty - HC). Standard HIPERLAN definiuje trzy rodzaje ramek:

- ramki danych - DT (ang. *DT-HCPDU*) - z jednostkami informacyjnymi podwarstwy MAC;
- ramki powiadomień - AK (ang. *AK-HCPDU*) - zawierające akceptację odbioru ramek DT;
- ramki CP przydziału do celów transmisji podkanałów 3 i 4 - CP (ang. *CP-HCPDU - Channel Permission*) - informujące stacje sąsiednie o pozwoleniu na wykorzystanie do celów transmisyjnych podkanałów oznaczonych w standardzie jako 3 i 4 (wykorzystywanych opcjonalnie).

Ramki DT i CP, przesyłane w sieci HIPERLAN, składają się z dwóch wyodrębnionych części, w których informacje binarne nadawane są z różnymi szybkościami:

- małą - w części *Low Bit Rate* (LBR) wynoszącą  $1.4706 \text{ Mb/s} \pm 15 \text{ b/s}$
- oraz
- dużą - w części *High Bit Rate* (HBR) wynoszącą  $23.5294 \text{ Mb/s} \pm 235 \text{ b/s}$

Ramki powiadomień AK zawierają jedynie część o małej (LBR) szybkości transmisji.

Funkcje transferu danych zapewnia przekaz ramek DT. Przygotowana przez użytkownika usług CAC jednostka HCS DU jest zaopatrzona między innymi w: priorytet dostępu (uzależniony od ważności informacji deklarowanej przez obiekt MAC oraz tzw. pozostałoego unormowanego czasu życia NRML) i adres stacji przeznaczenia (który może być indywidualny lub grupowy). Należy przy tym zwrócić uwagę na to, że użytkownik usług CAC może zainicjować kolejny przekaz HCS DU tylko wtedy, gdy wcześniejsza informacja została potwierdzona.

Indywidualna ramka DT musi być zawsze powiadomiona ramką AK przez obiekt HC będący adresatem DT. Tylko wtedy transmisja indywidualnej ramki DT (do adresata indywidualnego) może być uznana za udaną. Z kolei ramki DT z adresami grupowymi nigdy nie są potwierdzane ramkami AK i są zawsze traktowane jako przesłane udanie. Przekaz danych z obiektu HM do obiektu HCS może mieć miejsce po wygenerowaniu przez interfejs logiczny operacji podstawowej HC-SYNC.indication lub HC-FREE.indication.

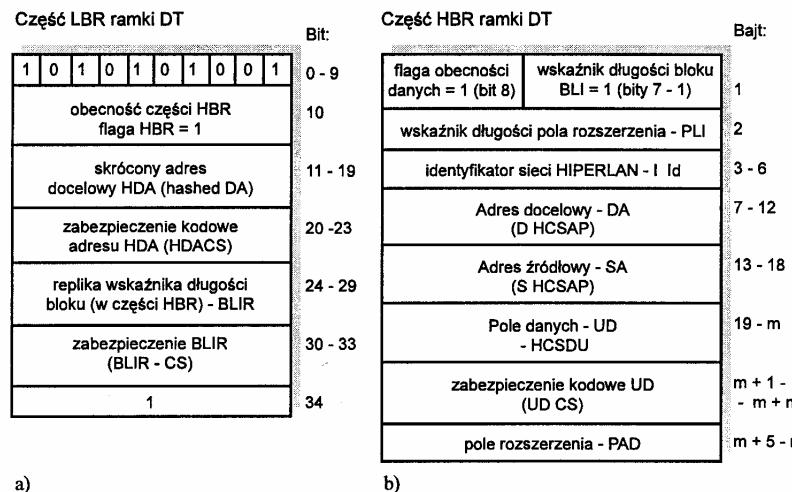
Struktura ramki DT pokazana jest na rysunku 5.24. Rysunek 5.24a ilustruje część LBR ramki, podczas gdy rysunek 5.24b prezentuje zawartość części HBR.

- Do zabezpieczania pól w części LBR stosowany jest kod cykliczny generowany przez wielomian  $G(x) = x^4 + x + 1$ . Z kolei część HBR

ramki DT (lub CP) zabezpieczona jest kodem generowanym przez wiele mian o postaci

$$\begin{aligned} G(x) = & x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} \\ & + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1 \end{aligned}$$

- Wskaźnik długości pola rozszerzenia PLI podaje długość dodatkowego ciągu bajtów - mogącą przyjmować wartości od 0 do 52 bajtów (por. IEEE 802.3);
- Pole BLI/BLIR sygnalizuje obecność w ramce DT określonej liczby 52 bajtowych bloków informacyjnych. Liczba bloków może się zmieniać od 1 do 47. Maksymalna długość pola danych ramki DT (HCSDU) nie może przekroczyć 2422 bajtów.

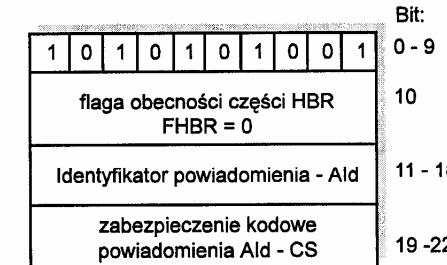


Rys. 5.24. Struktura ramki DT: a) część LBR ramki, b) część HBR ramki

Należy zwrócić uwagę na fakt, że warstwa fizyczna wprowadza dodatkowe istotne modyfikacje w strukturze transmitowanej ramki. Część HBR jest poprzedzana 450 bitowym ciągiem synchronizacyjnym (typu HBR). Zawartość HBR ramki jest też dodatkowo kodowana. Każdy 416 bitowy ciąg jest dzielony na 16 segmentów po 26 bitów, a każdy segment jest kodowany kodem BCH (31,26). W wyniku otrzymujemy 496 bitowe bloki danych.

Każda transmisja indywidualnej ramki DT musi być powiadomiona pozytywnie ramką AK (typu LBR). Zgodnie z protokołem HIPERLAN ramka AK-HCPDU musi być wysłana w ścisłe określonym czasie. Standard narzuca, by rozpoczęcie nadawania AK miało miejsce po czasie odpowiadającym czasowi trwania

$512 \pm 5$  okresów HBR (bitów typu HBR) - licząc od zakończenia odbioru ramki DT-HCPDU. Generowana przez obiekt HCS ramka AK zawiera tylko część LBR, o małej szybkości transmisji. Postać ramki AK ilustruje rysunek 5.25.



Rys. 5.25. Struktura ramki AK-HCPDU (ramka typu LBR)

#### 5.4.3 Algorytm niewymuszonego priorytetowego dostępu do medium - NPMA

Protokół HIPERLAN CAC przewiduje trzy procedury dostępu do kanału:

- procedurę dostępu do kanału wolnego,
- procedurę dostępu NPMA do kanału zajętego z synchronizowaniem się pracy stacji z końcem cyklu zajętości kanału oraz
- procedurę dostępu do kanału w przypadku tzw. „ukrytej eliminacji”.

##### Dostęp do kanału wolnego

Jeżeli stacja nie zaobserwuje aktywności w kanale wspólnym przez okres odpowiadający czasowi transmisji co najmniej 1800 bitów HBR, wówczas traktuje kanał jako wolny i rozpoczyna transmisję z pominięciem jakichkolwiek dodatkowych działań. Czas odpowiadający 1800 bitom HBR może być przy tym wydłużony o od 0 do 3 dodatkowych okresów, o długości 200 bitów HBR każdy.

##### Dostęp do kanału zajętego

Jeżeli stacja stwierdzi, że w kanale realizowana jest transmisja ramki bądź podejmowane są działania protokolarne zmierzające do jej realizacji, wówczas musi ona dokonać zsynchronizowania swoich procedur z końcem tzw. cyklu transmisyjnego, z dokładnością do  $\pm 10$  bitów HBR. W przypadku dużej intensywności zgłoszeń w pracy kanału wyróżniamy cykle transmisyjne. Każdy taki cykl składa się z trzech podstawowych faz:

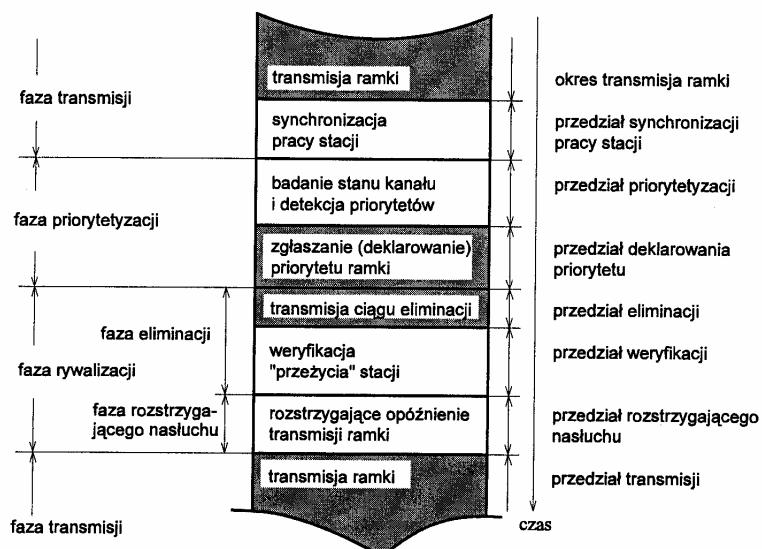
- fazy zgłaszania priorytetów i wyłaniania stacji (jednej lub kilku) o najwyższym priorytecie;
- fazy rywalizacji z wyłanianiem jednej (lub kilku) stacji "przeżywających" ten proces oraz

- fazy transmisji.

Stosowany przez podwarstwę CAC protokół nazywany jest **Niewymuszonym Priorytetowym Protokołem Dostępu do Kanału NPMA** (ang. *Non-preemptive Priority Multiple Access*).

Procedura NPMA zapewnia hierarchiczną niezależność dostępu do kanału ramkom o różnych priorytetach (zdefiniowanych przez HIPERLAN MAC). Protokół NPMA stanowi kombinację metody CSMA z algorytmami eliminacji i rozwiązywania zaistniałych konfliktów.

Dokonamy obecnie opisu kolejnych faz realizacji algorytmu dostępu do medium, pokazanych na rysunku 5.26.



Rys. 5.26. Ilustracja kolejnych faz algorytmu NPMA

#### Faza wyłaniania ramek o najwyższym priorytecie

Faza ta rozpoczyna się po zakończeniu cyklu transmisyjnego związanego z przesłaniem ramki.

1. Zakłada się istnienie  $m_{CP}$  klas priorytetów ponumerowanych od 0 do  $m_{CP} - 1$ ; przy czym 0 oznacza najwyższy priorytet dostępu.
2. W momencie rozpoczęcia się kolejnego cyku oś czasu dzielona jest na szczelin czasowe nazywane szczelinami priorytetyzacji ( $i_{PS}$ ).
3. Proces wyłaniania najwyższego priorytetu ramek odbywa się poprzez:
  - detekcję stanu kanału oraz

- deklarowanie priorytetów ramek.
4. Stacja mająca do przesłania ramkę o priorytecie  $n$  bada stan kanału (nasłuchiwanie) przez  $n$  pierwszych szczeleń priorytetyzacji ( $n * i_{PS}$ ). Jeżeli w tym czasie nie stwierdzi aktywności w kanale (oznacza to brak gotowych do transmisji ramek o priorytecie wyższym niż  $n$ ) stacja generuje ciąg sygnałów o czasie trwania  $i_{PA}$  (deklarując tym samym priorytet ramki). Inne stacje mające do przesłania ramki o priorytetach niższych niż  $n$  po usłyszeniu transmisji rezygnują z ubiegania się o dostęp do medium w danym cyklu.
  5. W ogólności, przynajmniej jedna spośród rywalizujących stacji pozostaje aktywna.

#### Faza rywalizacji o dostęp do kanału

Faza ta obejmuje dwa podstawowe okresy:

- okres eliminacji stacji oraz
- okres rozstrzygnięcia konfliktu.

1. Po zakończeniu fazy deklarowania priorytetów ma miejsce kolejna dyskretyzacja osi czasu i podział kanału w czasie na tzw. szczelin eliminacji ( $i_{ES}$ ). Stacje wyłonione w poprzedniej fazie, jako mające do przesłania ramki o najwyższym priorytecie, przesyłają ciągi (paczki) sygnałów eliminacji o czasach trwania będących wielokrotnością  $i_{ES}$ .
2. Długość ciągu eliminacji może zmieniać się od 0 do  $m_{ES}$  szczeleń eliminacji, zgodnie z rozkładem geometrycznym:

$$P_E^{(n)} = \begin{cases} P_E^n (1 - P_E) & ; 0 \leq n < m_{ES} \\ P_E^{m_{ES}} & ; n = m_{ES} \end{cases}$$

3. Proces eliminacji stacji z ubiegania się o dostęp jest rozstrzygany w sposób następujący: stacja po przesłaniu sygnału eliminacji o długości od 0 do  $m_{ES} * i_{ES}$  szczeleń czasowych, przechodzi w stan nasłuchu na okres  $i_{ESV}$ .
4. Jeżeli stacja po zakończeniu transmisji ciągu słyszy w okresie  $i_{ESV}$  inną transmisję, wówczas rezygnuje z ubiegania się o dostęp w danym cyklu. Stacja "przeżywa" fazę eliminacji wtedy i tylko wtedy, gdy po zakończeniu transmisji ciągu eliminacji stwierdza, że kanał jest wolny.
5. Czas trwania przedziału eliminacji jest wyznaczany poprzez czas trwania najdłuższego ciągu eliminacji. W ogólności przynajmniej jedna stacja wychodzi "zwycięsko" z opisanego powyżej procesu.

#### Ostatni rozstrzygający fragment rywalizacji o dostęp do medium przebiega w sposób następujący:

1. W dziedzinie czasu ma miejsce kolejna dyskretyzacja chwil dostępu do kanału i podział czasu pracy kanału na szczeleń  $i_{S}$ .

2. Stacje, które zwycięsko zakończyły okres rywalizacji mogą rozpoczęć transmisje ramek z opóźnieniem od 0 do  $m_{YS}$  szczezin  $i_{YS}$ . Opóźnienie w transmisji ma charakter losowy i jest opisane rozkładem równomiernym:

$$P_Y^{(n)} = 1 / (m_{YS} + 1); \quad 0 \leq n \leq m_{YS}$$

3. Algorytm rozstrzygającego opóźnienia transmisji wiąże się, podobnie jak poprzednie fazy protokołu dostępu, z badaniem stanu kanału przed rozpoczęciem transmisji ramki.
4. Stacja rozpoczyna transmisję ramki po losowym czasie opóźnienia wtedy i tylko wtedy, gdy żadna inna stacja nie rozpoczęła tego procesu wcześniej.
5. W ogólności przynajmniej jedna z rywalizujących stacji inicjuje transmisję, rozpoczynając tym samym ostatnią fazę CYKLU transmisyjnego, tj. fazę transmisji ramki.

#### Dostęp do kanału w przypadku tzw. „ukrytej” eliminacji stacji (ang. *Channel Access in Hidden Elimination Condition*)

Procedura ta może być stosowana w sieci, w której nie wszystkie stacje słyszą się wzajemnie. Stanowi ona uzupełnienie algorytmu dostępu do kanału zajętego. Podczas normalnej pracy sieci, po zsynchronizowaniu działań stacji z końcem cyklu transmisyjnego, rozpoczyna się faza zgłoszania priorytetów, a następnie faza rywalizacji, z wyłanianiem jednej (lub kilku) stacji przebywających ten proces. **Realizacja algorytmu „ukrytej” eliminacji ma miejsce, gdy stacja (lokalny obiekt HC) przegrywa rywalizację, lecz nie słyszy żadnej transmisji w kanale radiowym.** Stacja zakłada tym samym, że proces rywalizacji został „wygrany” przez stację znajdującą się poza zasięgiem jej słyszalności. Stacja przechodzi wówczas w stan tzw. „ukrytej” eliminacji, trwający 500 ms. Przejście do tego stanu ma miejsce również i wtedy, gdy po transmisji własnej ramki jednoadresowej np. DT-HCPDU (LBR-HBR HCPDU) stacja nie odbiera powiadomienia AK-HCPDU (LBR-HCPDU).

Licznik odmierzający czas przebywania w stanie „ukrytej” eliminacji jest ustawiany na wartość 500 ms po każdorazowej „porażce” stacji lub braku AK-HCPDU. Kolejne próby dostępu stacji do kanału, w stanie „ukrytej eliminacji”, są opóźniane o przedział czasu określany jako czas wstrzymywania (odłożenia) transmisji. Czas ten może trwać od 1 do  $m_{ss}$  ( $m_{ss} = 5$ ) szczezin jednostkowych, definiowanych jako szczezliny  $i_{ss}$  odłożonej transmisji. Po upływie czasu  $n_{ss}$  ( $i_{ss} \leq n_{ss} \leq m_{ss} i_{ss}$ ), przy braku transmisji w kanale, stacja podejmuje decyzję o próbie przesłania swojej ramki. Tym samym do sterowania dostępem stacji do kanału, w stanie „ukrytej eliminacji” (rywalizacji), używane są dwa liczniki, jeden - 500 ms, odmierzający czas pozostawania w tym stanie i drugi - odmierzający opóźnienia ewentualnych prób dostępu (o od 1 ms do 5 ms). Opóźnianie prób dostępu przez stację oznacza też, że nie uczestniczy ona w rywalizacji o prawo transmisji w każdym cyklu transmisyjnym, lecz włącza się do rywalizacji co pewien losowy przedział

czasu. Niekorzystny wpływ efektu stacji ukrytych na jakość pracy sieci ulega tym samym ograniczeniu. Wydłuża się jednakże opóźnienie w transmisji ramek.

#### Faza transmisji ramki

W czasie trwania tej fazy mogą mieć miejsce następujące działania podejmowane przez obiekty HC:

- transmisje ramek DT-HCPDV jednoadresowych i towarzyszące im transmisje powiadomień AK-HCPDU,
- transmisje ramek DT-HCPDU wieloadresowych (bez powiadomień AK),
- transmisje ramek CP-HCPDU z informacją o dostępności kanałów 3 i 4.

Zakładając jednoczesną pracę w sieci 256 stacji oraz ich rozlokowanie na obszarze o promieniu 50 m, standard HIPERLAN proponuje następujące wartości parametrów charakteryzujących kolejne fazy algorytmu NPMA, gwarantujące częstość kolizji ramek na poziomie poniżej 3.5%:

$m_{CP} = 5$  - zgodnie z liczbą priorytetów zdefiniowanych przez HIPER-LAN CAC (w zależności od ważności informacji i wartości tzw. znormalizowanego czasu życia ramki)

$i_{PS} = 168$  bitów HBR

$i_{PA} = 168$  bitów HBR

$P_E = 0.5$

$m_{ES} = 12$

$i_{ES} = 212$  bitów HBR

$i_{ESV} = 256$  bitów HBR

$m_{YS} = 9$

$i_{YS} = 168$  bitów HBR.

## 5.5 Systemy satelitarne VSAT

Sieci VSAT (ang. *Very Small Aperture Terminals*) to systemy łączności abonenckiej, w których końcowe urządzenia nadawczo-odbiorcze instalowane są bezpośrednio u abonentów. Można je traktować jako sieci wydzielone lub podsystemy komunikacyjne sieci rozległych, głównie sieci korporacyjnych.

Nazwa VSAT - *Very Small Aperture Terminal* - wiąże się z wykorzystaniem do celów łączności - między odległymi urządzeniami końcowymi, a stacją centralną sieci - małogabarytowych anten satelitarnych. Stacje końcowe tych systemów przekazują informacje cyfrowe za pośrednictwem kanałów satelitarnych do stacji centralnej, która może być np. węzłem komutacji pakietów.

Sieć VSAT może pracować w jednym z trzech trybów: trybie rozgłaszenia, gdy informacje przekazywane są ze stacji centralnej do stacji końcowych, w trybie

zbiorczym, gdy informacje przekazywane są ze stacji końcowych do stacji centralnej, bądź też trybie interaktywnym, w którym informacje przesyłane są między dowolnymi stacjami końcowymi VSAT.

Pierwsze systemy komunikacji satelitarnej uważane za sieci VSAT pojawiły się na początku lat osiemdziesiątych w USA. Były to sieci o konfiguracji gwiazdy, przeznaczone do rozgłaszenia informacji. Stacje końcowe wyposażone były w anteny o średnicy 0,6 metra, a prędkość transmisji od stacji centralnej do stacji końcowych wynosiła od 300 do 9600 b/s.

Od tego czasu, szczególnie w USA i Kanadzie, zaczęły powstawać podobne sieci. Europa początkowo nieufnie odnosila się do tej satelitarnej nowości. Gwałtowny wzrost zainteresowania tym typem sieci spowodował, że pod koniec lat 80-tych systemy VSAT stały się dojrzałą technologią i zaczęły powoli pojawiać się w Europie. Ten szybki rozwój został w dużej mierze wywołany przez:

- wymagania rynku; szczególnie przez powstanie sieci sklepów i systemów dystrybucji towarów o dużej liczbie oddziałów,
- liberalizację przepisów wykorzystania łączysatelarnych,
- rozwój techniki satelitarnej.

**Sieci satelitarne VSAT charakteryzują się tym, że :**

- są to z reguły systemy zamknięte, przeznaczone dla specjalizowanych aplikacji, używane zarówno do rozgłaszenia, zbierania jak i wymiany informacji,
- stacje końcowe są instalowane bezpośrednio na terenie użytkownika,
- mają najczęściej architekturę gwiazdy, zawierającą jedną stosunkowo dużą stację centralną zwaną Hubem i wiele rozproszonych stacji końcowych,
- szybkość transmisji danych jest z reguły mniejsza niż 2 Mb/s,
- stacje końcowe wyposażone są w anteny nadawczo-odbiorcze o małych średnicach, normalnie nie przekraczających 2,5m.

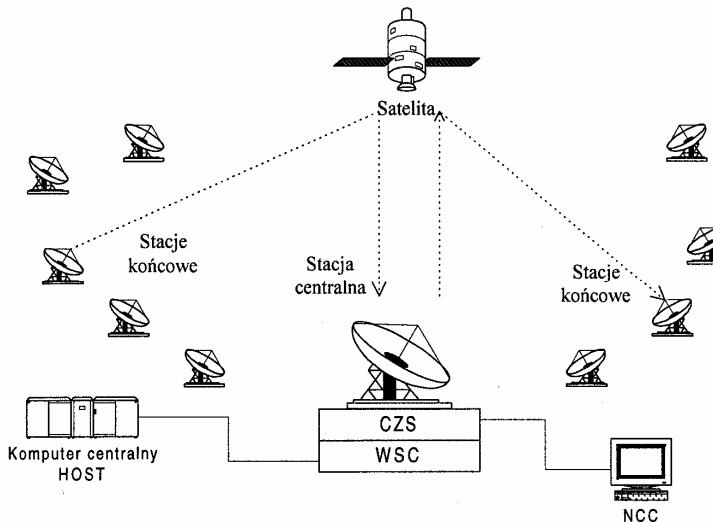
Należy tutaj zaznaczyć, że systemy satelitarne przeznaczone do odbioru telewizji publicznej nie są traktowane jako sieci VSAT mimo, że zwykle odpowiadają po-wyższej charakterystyce.

### 5.5.1 Konfiguracje fizyczne sieci VSAT

Ze względu na sposób organizacji połączeń fizycznych w sieci, wyróżnić można dwie podstawowe konfiguracje sieci satelitarnych VSAT :

- sieci VSAT o architekturze gwiazdy (ang. *star topology*),
- sieci VSAT o architekturze oczkowej (ang. *mesh topology*).

W chwili obecnej większość funkcjonujących systemów VSAT zbudowanych jest zgodnie z architekturą gwiazdy (patrz rysunek 5.27). W takiej sieci połączenia komunikacyjne odbywają się pomiędzy stacją centralną, często nazywaną Hubem, i pewną, zwykle dużą, liczbą stacji końcowych.



Rys. 5.27. Sieć VSAT o architekturze gwiazdy: WSC - wyposażenie stacji centralnej (ang. *Hub baseband equipment*), CZS - centrum zarządzania siecią (ang. *Network Control Center*)

Sieć zarządzana jest z jednego miejsca, zwanego centrum zarządzania siecią CZS (ang. *Network Control Center*). Centrum zarządzania siecią CZS najczęściej umiejscowione jest w stacji centralnej. Do podstawowych zadań CZS należy :

- konfigurowanie stacji końcowych VSAT,
- taryfikacja ruchu w sieci,
- monitorowanie stanu sieci VSAT oraz monitorowanie stanów alarmowych stacji końcowych VSAT,
- konfigurowanie połączeń między elementami systemu,
- wprowadzanie do bazy danych wszystkich informacji dotyczących aktualnej konfiguracji sieci oraz informacji o podłączonych do sieci użytkownikach,
- prowadzenie statystyk dotyczących natężenia ruchu w sieci oraz stanów alarmowych pojawiających się w sieci VSAT.

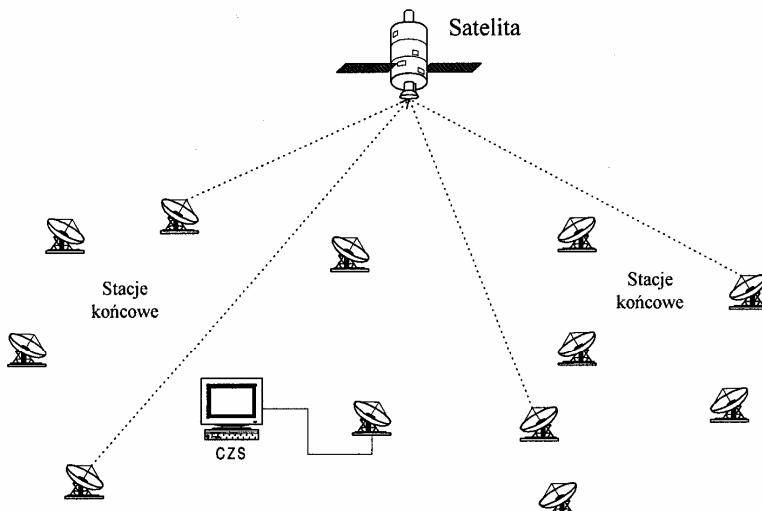
Stacja centralna organizuje, za pomocą posiadanego sprzętu i oprogramowania WSC (ang. *Hub Baseband Equipment*), komunikację w sieci VSAT. Jednym z ważniejszych elementów WSC jest system komutacyjny odpowiedzialny za przekazywanie (routing) pakietów danych, przesyłanych ze stacji końcowych. W sieciach VSAT występuje tylko jeden węzeł komutacji pakietów zlokalizowany w stacji centralnej.

W sieciach o konfiguracji gwiazdy można prowadzić połączenia jedno- lub dwukierunkowe pomiędzy Hubem (stacją centralną) i stacjami końcowymi. Jest także

możliwe dokonywanie połączeń pomiędzy stacjami końcowymi. Odbywa się to jednak zawsze poprzez stację centralną. Połączenia pomiędzy stacjami końcowymi, a stacją centralną, wymagają tylko jednego przejścia sygnału przez satelitę, natomiast połączenia pomiędzy odległymi stacjami końcowymi - dwóch.

Trzeba zaznaczyć, że większość (ponad 90%) istniejących obecnie systemów VSAT, to sieci o architekturze gwiazdy.

*W sieciach VSAT o konfiguracji oczkowej (patrz rysunek 5.28) mamy do czynienia z bezpośrednimi połączeniami pomiędzy stacjami końcowymi VSAT.*



Rys. 5.28. Sieć VSAT o architekturze oczkowej: CZS - centrum zarządzania siecią (ang. *Network Control Center*)

W architekturze tej nie ma więc stacji centralnej, pośredniczącej w komunikacji pomiędzy stacjami VSAT, dlatego też sieci o takiej konfiguracji często nazywane są sieciami VSAT bez stacji Hub (ang. *hubless VSAT networks*). Centrum zarządzania siecią CZS podłączone jest do wybranej stacji końcowej.

Podstawowym obszarem zastosowań sieci VSAT o konfiguracji oczkowej jest interakcyjna transmisja glosu i obrazu; przede wszystkim ze względu na mniejsze opóźnienia transmisji sygnału w porównaniu do sieci VSAT o architekturze gwiazdy (wszystkie połączenia wymagają tylko jednego przejścia sygnału przez satelitę).

### 5.5.2 Organizacja transmisji w sieci VSAT

Ze względu na sposób organizacji połączeń logicznych w sieci, wyróżnić można trzy podstawowe rodzaje topologii sieci satelitarnych VSAT:

- sieci rozsiewcze (ang. *broadcast networks*),
- sieci łączności bezpośredni (ang. *point-to-point networks*),
- sieci interakcyjne (ang. *two-way interactive networks*).

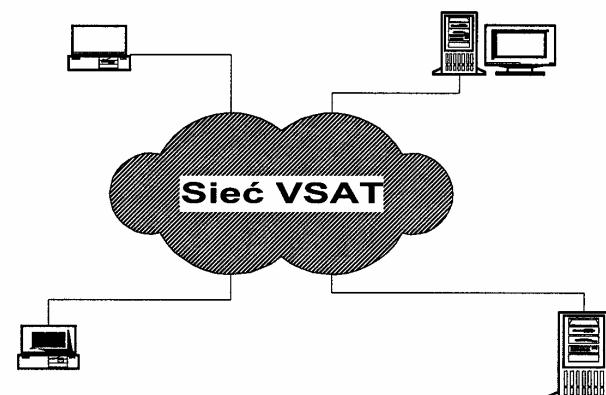
*Rozsiewcze sieci VSAT charakteryzują się prowadzeniem jednokierunkowej komunikacji od stacji centralnej (Huba), do pewnej (zwyczaj duzej) liczby stacji końcowych.* Sieci rozsiewcze budowane są w oparciu o systemy VSAT o architekturze gwiazdy.

*W sieciach łączności bezpośredni komunikacja jest prowadzona pomiędzy dowolnymi odległymi stacjami końcowymi.* Może się to odbywać zarówno bez udziału stacji centralnej - w sieciach VSAT o architekturze oczkowej - jak i za pośrednictwem stacji centralnej - w sieciach VSAT o architekturze gwiazdy.

*Interakcyjne sieci VSAT* są obecnie najczęściej spotykane. *Korzystając z architektury gwiazdy, w sieciach VSAT o tej topologii prowadzona jest dwukierunkowa komunikacja pomiędzy stacją centralną (Hubem), a stacjami końcowymi. Możliwa jest także komunikacja pomiędzy odległymi stacjami końcowymi, zawsze jednak odbywa się to za pośrednictwem stacji centralnej.*

### 5.5.3 Architektura komunikacyjna sieci VSAT

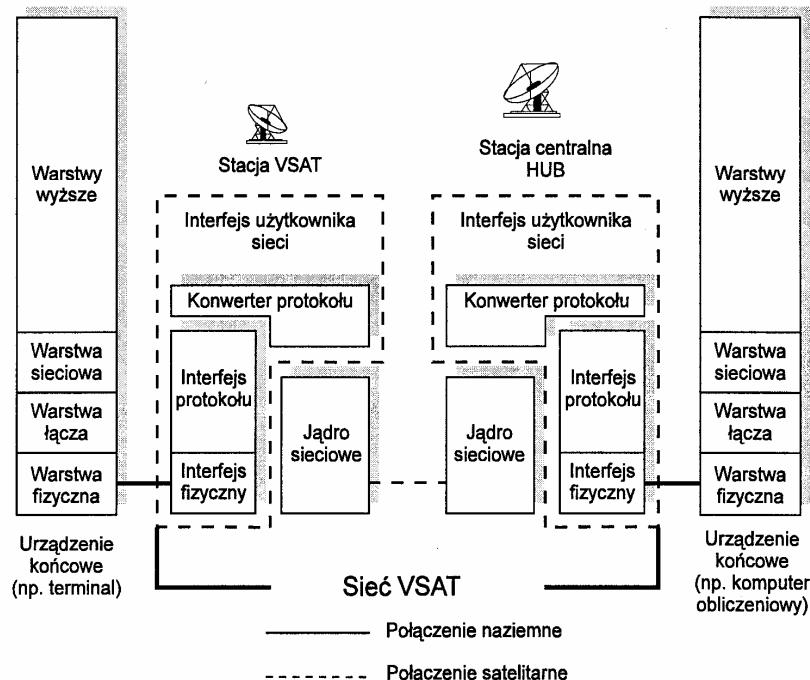
Sieć VSAT można traktować jako podsystem komunikacyjny (patrz rysunek 5.29), który jest w stanie połączyć dwie dowolne stacje VSAT (węzły) za pomocą kanału satelitarnego.



Rys. 5.29. Model komunikacyjny sieci VSAT

Do stacji końcowej sieci VSAT może być dołączone dowolne urządzenie teleinformatyczne lub zespół takich urządzeń, wyposażonych w podzespoły i oprogramowanie umożliwiające wymianę informacji cyfrowych, zgodnie z protokołem przyjętym w danym systemie VSAT.

W budowie każdej stacji VSAT (końcowej jak i centralnej) możemy wyodrębnić dwa podstawowe komponenty strukturalne (patrz rysunek 5.30).



Rys. 5.30. Schemat blokowy architektury komunikacyjnej sieci VSAT

- interfejs użytkownika sieci (ang. *User Network Interface*) – odpowiedzialny za podłączanie urządzeń końcowych do sieci VSAT,
- jądro sieciowe (ang. *Network Kernel*) - odpowiedzialne za wewnętrzną komunikację w sieci VSAT.

### Interfejs użytkownika sieci VSAT

Interfejs użytkownika sieci VSAT, nazywany także interfejsem sieci VSAT, pozwala podłączać do sieci VSAT urządzenia końcowe użytkowników, niezależnie od użytego w sieci VSAT protokołu komunikacyjnego. Każdy interfejs sieci VSAT zbudowany jest z trzech zasadniczych części:

- interfejsu fizycznego (ang. *physical interface*),
- interfejsu protokołu (ang. *protocol interface*),
- konwertera protokołu (ang. *gateway*).

*Interfejs fizyczny* zapewnia fizyczne połączenie pomiędzy urządzeniem końcowym użytkownika, a siecią VSAT. Każda stacja VSAT ma zazwyczaj kilka niezależnych i konfigurowalnych interfejsów fizycznych, najczęściej spotykanych standardów.

*Interfejs protokołu* pozwala podłączać do sieci VSAT urządzenia pracujące pod kontrolą różnych protokołów. Funkcjonalnie interfejs protokołu posiada logikę warstwy łącza danych i sieciowej konkretnego protokołu. Każdy interfejs protokołu jest zdalnie konfigurowalny ze strony stacji centralnej. Większość systemów VSAT posiada przynajmniej kilka rodzajów interfejsów protokołu; najczęściej są to :

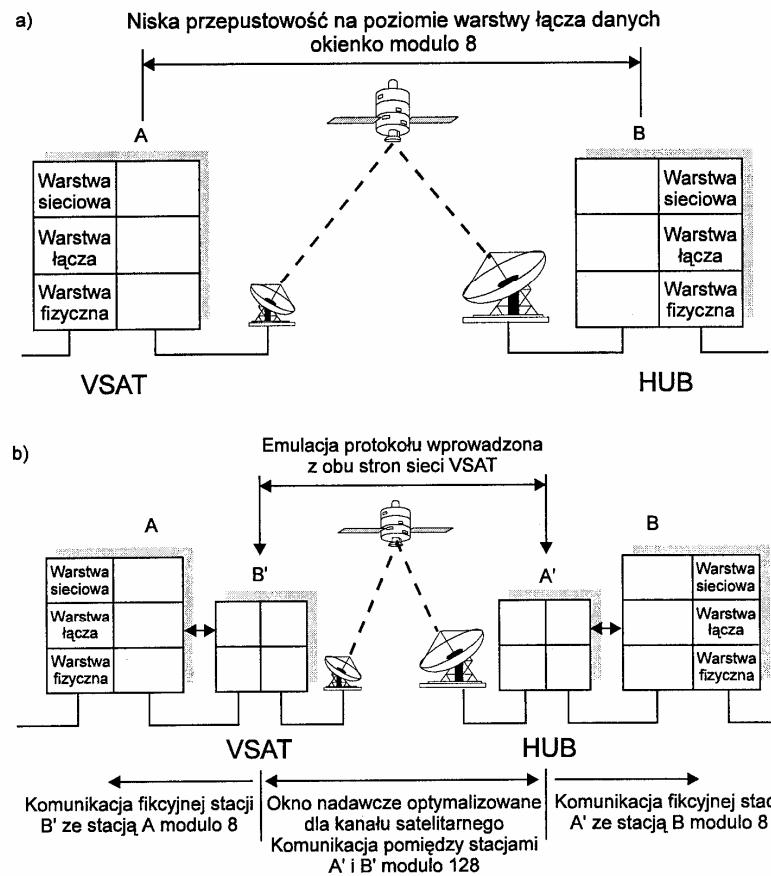
- interfejs protokołu BiSync,
- interfejs protokołu SDLC,
- interfejs protokołu X.25,
- interfejs protokołu Frame Relay.

Każdy interfejs sieci VSAT ma swój własny *konwerter protokołu*, którego zadaniem jest dokonywanie konwersji pomiędzy protokołem komunikacyjnym tegoż interfejsu, a wewnętrznym protokołem komunikacyjnym sieci VSAT. Ważną funkcję realizowaną przez konwerter protokołu jest tzw. emulacja protokołów.

### Emulacja protokołów

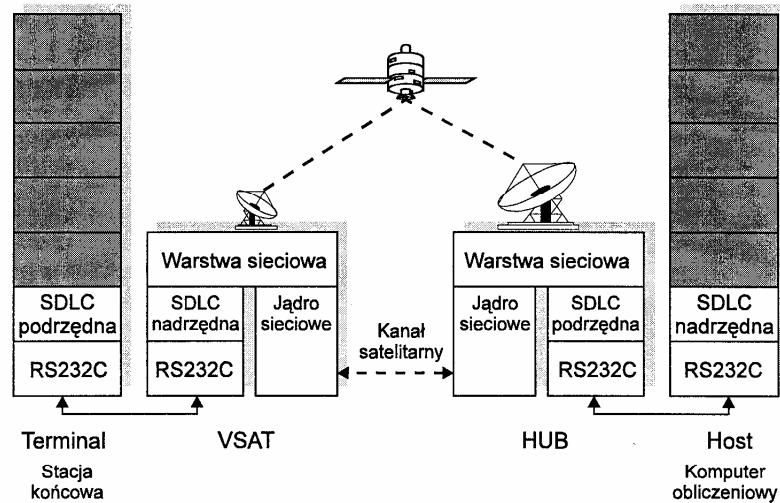
Pierwszy rodzaj emulacji protokołów dokonywanej przez konwerter protokołu wiąże się z korzystaniem z tzw. okienka nadawczego w istniejących protokołach komunikacyjnych.

Większość stosowanych protokołów łącza danych, w celu zapewnienia niezawodnej komunikacji po łączu fizycznym, używa potwierdzeń wysyłanych ramek. Stacja nadająca nie może wysłać więcej niż pewną ustaloną liczbę niepotwierdzonych ramek (jest to tzw. okienko nadawcze). W sieciach naziemnych wartość ta jest z reguły mała (np. 7), natomiast w sieciach satelitarnych, takich jak VSAT, ze względu na duże opóźnienia transmisji danych w kanale satelitarnym, protokół łącza danych z małym okienkiem nadawczym może stać się nieefektywny (zależy to od długości pakietów i jakości łącza satelitarnego). Dlatego też może się okazać, że potrzebne jest większe okienko nadawcze, niż to które występuje w protokole komunikacyjnym sieci naziemnej. Potrzebny jest zatem moduł oprogramowania, który pozwoli na zwiększenie rozmiaru okienka nadawczego do odpowiedniego poziomu, w sposób przezroczysty dla użytkowników sieci VSAT. Rolę tę spełnia konwerter protokołu wysyłając do stacji nadawczej „fałszywe” potwierdzenia odbioru ramek, „pozostawiając” sieci VSAT odpowiedzialność za właściwe ich dostarczenie do adresata. Istotę tej emulacji ilustruje rysunek 5.31, na którym przedstawiono schematycznie komunikację poprzez sieć VSAT pomiędzy stacjami A i B w sytuacji, gdy brak jest emulacji okienka nadawczego (rysunek 5.31a) i gdy ona występuje (rysunek 5.31b).



Rys. 5.31. Ilustracja emulacji okienka nadawczego

Drugi rodzaj emulacji protokołów zachodzi w przypadku podłączenia do sieci VSAT urządzeń końcowych pracujących w tzw. trybie niezrównoważonym (np. jeden z trybów pracy protokołów HDLC lub SDLC). W trybie tym stacja podrzędna (ang. *slave*) nie może rozpoczęć transmisji swoich danych przed otrzymaniem pozwolenia na nadawanie od stacji nadzornej (ang. *master*). Ze względu na duże opóźnienie transmisji w kanale satelitarnym, oczekiwanie na pozwolenie od stacji nadzornej przez stację podrzędną powodowałoby niezadowalającą pracę sieci. W tym przypadku emulacja polega na tym, że konwerter protokołu „imituje” stację nadzorną od strony stacji podrzędnej wysyłając jej pozwolenia na transmisję danych oraz „imitując” stację podrzędną od strony stacji nadzornej, wysyłając dane dopiero po otrzymaniu pozwolenia na nadawanie.



Rys. 5.32. Ilustracja emulacji protokołu pracującego w trybie niezrównoważonym

Rysunek 5.32 ilustruje przykładową komunikację pomiędzy terminaliem, a hostem (komputerem obliczeniowym) podłączonym do stacji centralnej. Komunikacja pomiędzy terminaliem, a stacją VSAT, odbywa się za pośrednictwem protokołu SDLC. Protokół SDLC definiuje komunikację pomiędzy stacją nadzorną i podrzędną. Stacja podrzędna nie może transmitować danych przed otrzymaniem pozwolenia na nadawanie od stacji nadzornej, gdzie wymiana informacji odbywa się w trybie przepływu (ang. *polling*). Aby uniknąć długiego czasu oczekiwania przez stację podrzędną na pozwolenie transmisji, stacja VSAT „imituje” przed terminaliem stację nadzorną i sama okresowo wysyła mu pozwolenia na nadawanie. Natomiast stacja centralna (Hub) „imituje” przed stacją nadzorną stację podrzедną, tzn. przesyła do niej dane tylko wtedy, gdy otrzyma pozwolenie na nadawanie.

### Jądro sieciowe

Jądro sieciowe decyduje o sposobie przesyłania danych wewnętrz sieci VSAT, tj. poprzez kanał satelitarny. Zawiera ono zestaw protokołów i struktur danych zapewniających bezstratną i efektywną komunikację w kanale satelitarnym. Podstawowe elementy jądra sieciowego to :

- protokół dostępu do satelity,
- mechanizm adresowania pakietów,
- procedury przeciwdziałania przeciążeniom w kanale satelitarnym,
- mechanizm routingu pakietów,

- mechanizm zarządzania siecią.

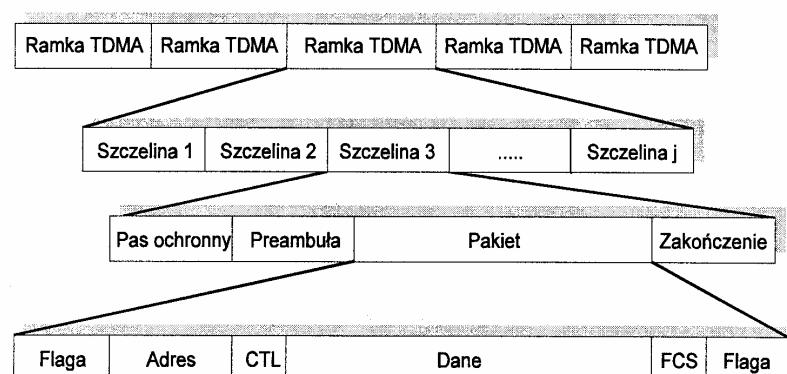
Większość systemów VSAT jest zaprojektowanych jako sieci pakietowe. W przypadku sieci o architekturze gwiazdy, występuje jeden centralny węzeł komutacji pakietów, znajdujący się w stacji centralnej (Hub).

#### 5.5.4 Schemat komunikacji w typowej sieci VSAT o architekturze gwiazdy

Sposób prowadzenia komunikacji pomiędzy stacjami końcowymi, a stacją centralną oraz pomiędzy stacją centralną i stacjami końcowymi zależy od architektury sieci VSAT. Poniżej prezentujemy rozwiązanie komunikacyjne dla typowej sieci VSAT o architekturze gwiazdy.

##### Komunikacja w kanale od stacji końcowych do stacji centralnej

Pakiety danych przesyłane od stacji końcowych do stacji centralnej współdziela kanał satelitarny. Czas pracy kanału podzielony jest na ramki TDMA o jednakowej długości (patrz rysunek 5.33). Ramki TDMA dzielone są z kolei na określoną liczbę szczelin czasowych. Stacje końcowe transmitują swoje pakiety korzystając z tych szczelin. Sposób przydziału szczelin stacjom zależy od stosowanego w danym systemie VSAT protokołu wielodostępu. Pomiędzy kolejnymi szczelinami czasowymi przewidziane są też odstępy bezpieczeństwa (pasy ochronne). Każda szczelina czasowa rozpoczyna się i kończy unikatowymi ciągami wzorcowymi (preamble i zakończenie). Zasadnicza część szczeliny pozwala na umieszczenie w niej pakietu (pakietów) przesyłanego (przesyłanych) przez stacje końcowe.

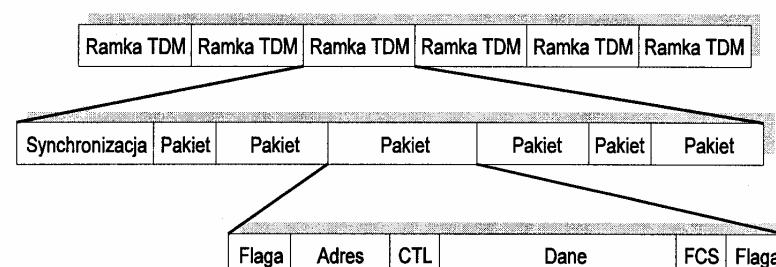


Rys. 5.33. Format danych przesyłanych w kanale od stacji końcowych do stacji centralnej

Każdy pakiet (ramka) rozpoczyna się i kończy pewną charakterystyczną sekwencją bitów (Flagą). Adres identyfikuje nadawcę pakietu. Pole kontrolne CTL określa rodzaj pakietu. Pole FCS stanowi zabezpieczenie kodowe pakietu. Pole danych (Dane) jest częścią transmitowanej informacji.

##### Komunikacja w kanale od stacji centralnej do stacji końcowych

Stacja centralna przesyła dane do stacji końcowych stosując technikę zwielokrotnienia czasowego TDM (patrz rysunek 5.34).



Rys. 5.34. Format danych przesyłanych w kanale od stacji centralnej do stacji końcowych

Cały kanał podzielony jest więc na ramki czasowe TDM, których początki wyznaczone są przez pojawianie się ciągów synchronizacyjnych. Pakiety danych przesyłane do stacji końcowych mogą być różnej wielkości. Ich początki i końca są wyróżnione flagą, czyli unikatową sekwencją bitów. Adres zawarty w pakiecie identyfikuje stację, dla której jest przeznaczony. Stacje odbierają pakiety adresowane tylko do nich. Stosując odpowiednią metodę adresowania grupowego można też rozsyłać pakiety do wszystkich lub wybranej grupy stacji końcowych. CTL jest polem kontrolnym określającym rodzaj pakietu. Pole FCS jest zabezpieczeniem kodowym pakietu. Pole danych (Dane) jest „porcją” transmitowanej informacji.

##### 5.5.5 Obszary zastosowań sieci VSAT i ich przykładowe aplikacje

W pierwszym okresie swojego rozwoju sieci satelitarne VSAT były używane przede wszystkim do zapewnienia transmisji danych grupie użytkowników, w ramach sieci prywatnej. W ciągu lat 80-tych zastosowania sieci VSAT uległy znacznemu rozszerzeniu. Służą one obecnie nie tylko do tworzenia sieci prywatnych, ale także sieci publicznych, świadczących przede wszystkim usługi w zakresie transmisji danych, lecz również w zakresie telefonii i faksymile. Przykłady zastosowań sieci VSAT ilustruje tabela 5.1.

Tabela 5.1. Obszary zastosowań sieci satelitarnych VSAT

Sieci teleinformatyczne z przetwarzaniem wsadowym i interakcyjnym
transakcje handlowe weryfikacje kart kredytowych systemy informacyjne typu pytanie - odpowiedź rezerwacja biletów usługi bankowe i finansowe wsadowe przetwarzanie plików
Sieci nadzoru, sterowania i pozyskiwania danych
nadzór i monitorowanie ropociągów, gazociągów itp. zbieranie informacji meteorologicznych, sejsmologicznych itp.
Sieci poczty elektronicznej
faksymile transfer plików
Sieci telekonferencyjne
skomprymowana transmisja sygnałów wizyjnych cyfrowa transmisja dźwięku rozsiewcza transmisja analogowych sygnałów wizyjnych
Transmisja porozumiewawcza
szbka transmisja danych transmisja obrazów z dużą rozdzielczością komunikacja specjalna w stanach awaryjnych
Sieci rozsiewcze
dystrybucja danych informacje giełdowe wyniki wyścigów konnych, loterii, gier liczbowych itp.
Sieci telekomunikacyjne o małym ruchu
krajowe sieci telekomunikacyjne i teleinformatyczne wiejskie sieci telekomunikacyjne dedykowane usługi telefoniczne i transmisji danych satelitarna służba reporterska

Lista instytucji zainteresowanych sieciami VSAT jest szeroka i obejmuje :

- banki oraz instytucje finansowe,
- urzędy administracji państowej,
- towarzystwa ubezpieczeniowe,
- agencje turystyczne,
- agencje reklamowe,
- agencje informacyjne,
- sieci sklepów.

Tabela 5.2. Parametry typowych sieci VSAT

	Produkt 1	Produkt 2	Produkt 3	Produkt 4	Produkt 5	Produkt 6
Pasmo częstotliwości	14/10-12	14/10-12	6/4 lub 14/10-12	6/4	14/10-12	14/10-12
Rozmiar anteny [ m ]	1.2, 1.8, 2.4	1.2, 1.8, 2.4	1.2, 1.8	1.1, 1.8	1.2, 1.8, 2.4	1.2, 1.8, 2.4
Protokół wielodostępu	P.ALOHA	S ALOHA kanaly de-dykowane	S ALOHA rezerwacja	CDMA	S ALOHA DA/TDMA	Adaptacyjny TDMA
Przepustowości kanałów [kb/s] do stacji Hub / od stacji Hub	35/512	56/256	64/256	9.6/153.6	128/512	56/56
Rodzaj transmitowanych danych	Dane, obraz	Dane, obraz, dźwięk	Dane, obraz	Dane	Dane, obraz, dźwięk	Dane, obraz
Interfejsy przyłącza	SDLC BISYNC	X.25, SDLC	X.25, SDLC	ASYNC, SDLC, TINET, BISYNC	SDLC, TINET, BISYNC	X.25, SDLC, ASYNC

W tabeli 5.2 zaprezentowano przykłady typowych sieci VSAT przeznaczonych do interaktywnej wymiany informacji pomiędzy odległymi stacjami końcowymi lub pomiędzy stacjami końcowymi, a stacją centralną. Do typowych aplikacji VSAT należą:

- Rozgłaszczenie danych: najbardziej rozpowszechnionym typem aplikacji jednokierunkowej znajdującej zastosowanie w sieciach VSAT jest rozgłaszczenie informacji cyfrowych (ang. *data distribution*) od stacji centralnej do wszystkich, lub do pewnej grupy stacji końcowych. Typowe rozwiązania sieci VSAT wykorzystujące ten typ przekazu danych, to systemy służące do rozpowszechniania informacji agencjnych, wiadomości giełdowych, prognoz pogody, danych komputerowych, itp.
- Rozgłaszczenie obrazu: przekazywanie obrazów telewizyjnych w sieciach VSAT jest ograniczone do transmisji dla celów biznesu, z wyłączeniem telewizji publicznej. Systemy tego typu (tj. telewizja publiczna) nie należą do klasy VSAT. Transmisja sygnału telewizyjnego może odbywać się w postaci cyfrowej (jako normalna transmisja danych) lub w postaci analogowej (jako dodatkowa funkcja realizowana przez stację końcową VSAT).
- Zbieranie danych: stacje końcowe VSAT mogą także służyć do jednokierunkowego przekazywania informacji do stacji centralnej. Mamy wówczas do czynienia z sytuacją odwrotną do rozgłaszczenia danych. Trzeba jednak zaznaczyć, że w rzeczywistych implementacjach sieci VSAT stacje końcowe są zwykle „zmuszone” do odbierania informacji od stacji

- centralnej (np. sygnałów synchronizacyjnych). Dlatego też zbieranie danych nie jest najbardziej typową aplikacją jednokierunkową.
- Przekaz danych: transmisja danych (ang. *data transfer*) jest w chwili obecnej najbardziej rozpowszechnioną dwukierunkową aplikacją występującą w sieciach VSAT. Transmisja danych może odbywać się zarówno pomiędzy stacjami końcowymi, a stacją centralną, jak i pomiędzy odległymi stacjami końcowymi.
  - Przekaz głosu i telefonia: chociaż tradycyjna usługa telefoniczna nie jest typową aplikacją w sieciach VSAT, to możliwe jest (i często realizowane w praktyce) tworzenie prywatnych łącz telefonicznych w ramach sieci. Można to zrealizować jako:
  - Transmisję głosu w postaci analogowej w wydzielonym kanale o odpowiedniej przepustowości SCPC (ang. *Single Channel Per Carrier*),
  - Transmisję głosu zakodowanego w postaci cyfrowej, jako normalną transmisję danych w sieci,
  - Videokonferencje: rozwój technik kompresji obrazu pozwolił na pojawienie się w sieciach satelitarnych VSAT aplikacji polegających na interaktywnej wymianie obrazu i dźwięku (videokonferencje). Szybkości transmisji wykorzystywane w tych aplikacjach to: 56/64 kb/s, 112/128 kb/s, 384 kb/s, 738 kb/s, aż do 1.544/2.048 Mb/s. Najczęściej używa się przy tym kanałów o szybkości 384 kb/s, gwarantujących kompromis pomiędzy jakością obrazu a kosztem transmisji.

### 5.5.6 Algorytmy dostępu do kanału satelitarnego

W systemach VSAT wykorzystywane są trzy podstawowe techniki zapewniające wielodostęp do kanału satelitarnego. Są to:

- wielodostęp z podziałem częstotliwości FDMA (ang. *Frequency Division Multiple Access*),
- wielodostęp z podziałem czasu TDMA (ang. *Time Division Multiple Access*),
- wielodostęp z podziałem kodowo-adresowym CDMA (ang. *Code Division Multiple Access*).

Wszystkie one polegają na odpowiednim podziale posiadanych zasobów transmisyjnych systemu. Idea współdzielenia zasobów transmisyjnych rodzi natychmiast pytanie o zasadę (algorytm) przydziału zasobów poszczególnym użytkownikom. W praktyce wyróżnia się trzy klasy algorytmów (protokołów) dostępu do podkanałów czasowych, częstotliwościowych lub czasowo-częstotliwościowych. Są to:

- metody stałego przydziału (ang. *Fixed Assignment Multiple Access*),
- metody losowego przydziału (ang. *Random Assignment Multiple Access*),
- metody przydziału na żądanie (ang. *Demand Assignment Multiple Access*).

Dobór właściwej metody przydziału prawa dostępu do kanału powinien być uzależniony od :

- statystycznej charakterystyki ruchu w sieci,
- dopuszczalnego maksymalnego opóźnienia transmisji,
- żądanego poziomu wykorzystania zasobów,
- kosztu implementacji i utrzymania.

Parametry typowych algorytmów dostępu do kanału satelitarnego, stosowanych w systemach VSAT, podane są w tabeli 5.3.

Tabela 5.3. Charakterystyka wybranych protokołów wielodostępu

Protokół wielodostępu	Maksymalne wykorzystanie kanału	Opóźnienie	Koszt implementacji protokołu	Typowe aplikacje	Uwagi
<b>Algorytmy stałego przydziału zasobów</b>					
TDMA	0.7 - 0.8	średnie - wysokie	średni	głos, obraz, transfer plików	Opóźnienie rośnie szybko ze wzrostem liczby stacji
FDMA/SCPC	0.7 - 0.8	średnie	bardzo niski	głos, obraz	Dobry tylko dla stacji o dużym ruchu
<b>Algorytmy losowego przydziału zasobów</b>					
P ALOHA	0.13 - 0.18	niskie	bardzo niski	transakcje, zapytania	Najprostszy protokół rywalizacyjny. Dobry dla stacji generujących wiadomości o zmiennej długości
S ALOHA	0.25-0.368	niskie	niski - średni	transakcje, zapytania	Najprostszy protokół szczeniowy. Dobry dla stacji generujących pojedyncze pakiety o stałej długości
SREJ-ALOHA	0.2 - 0.3	niskie	niski	transakcje	Dobry dla stacji generujących wiadomości o zmiennej długości.
S ALOHA z algorymem drzewiastym rozwiązywania kolizji : TREE-CRA	0.43 - 0.49	średnie	średni - wysoki	transakcje	Dobry dla stacji generujących pakiety o stałej długości.
CDMA	0.1 - 0.4	bardzo niskie	średni	transakcje, głos, obraz	Oferuje niskie opóźnienia. W większości implementacji wymaga FEC.

Tabela 5.3. Charakterystyka wybranych protokołów wielodostępu (c.d.)

Protokół wielodostępu	Maksymalne wykorzystanie kanału	Opóźnienie	Koszt implementacji protokołu	Typowe aplikacje	Uwagi
<b>Algorytmy przydziału rezerwacyjnego</b>					
SRUC RAN	0.6 - 0.9	średnie - wysokie	wysoki	transfer plików, transakcje	Dla ruchu o małym natężeniu występują małe opóźnienia w transmisji pakietów.
<b>Algorytmy przydziału zasobów na żądanie</b>					
DAMA/FDMA DAMA/TDMA	0.6 - 0.8	wysokie - średnie		transfer plików, głos	Duże opóźnienia transmisji pakietów z powodu rezerwacji.

#### 5.5.6.1 Metody stałego przydziału zasobów

Metody stałego przydziału polegają na przyporządkowaniu na stałe poszczególnym stacjom VSAT pewnej ilości zasobów. Może to polegać na przeznaczeniu na wyłączny użytk stacji VSAT kanału FDMA lub pewnej liczby szczelin czasowych TDMA. Rozwiążanie to jest dobre w sytuacji, gdy mamy do czynienia z generowaniem przez stacje ruchu ciągłego o ustalonej wielkości. W przypadku, gdy generowany ruch ma postać paczkową - „porowatą” o zmiennej w czasie intensywności, metoda stałego przydziału staje się nieefektywna ze względu na okresy niewykorzystania przydzielonych zasobów. Metody stałego przydziału podkanali stosowane są przede wszystkim w sieciach VSAT o architekturze oczkowej.

Typowe protokoły wielodostępu korzystające z metody stałego przydziału, występujące w praktycznych instalacjach sieci VSAT, to: TDMA i FDMA/SCPC (patrz tabela 5.3).

#### 5.5.6.2 Metody losowego przydziału zasobów

Metody losowego przydziału (zwane także protokołami lub algorytmami typu ALOHA) charakteryzują się tym, że stacje końcowe VSAT korzystają z tego samego kanału transmisyjnego (zwykle czasowego) w sposób losowy. Jeżeli w trakcie transmisji danych z jednej stacji, transmisję rozpoczęte także inną (inne) stacją (stacjami), wówczas będziemy mieli do czynienia z ich kolizją i realizowane transmisje będą niedane. Metody losowego przydziału stosowane są bardzo często w sieciach VSAT o architekturze gwiazdy. Algorytmy te są proste w implementacji i przy małym ruchu charakteryzują się małymi opóźnieniami w transmisji; przy średnim i dużym ruchu mogą być jednakże niestabilne. Istnieje bardzo wiele protokołów korzystających ze schematu typu ALOHA (patrz tabela 5.3). Najczęściej w sieciach VSAT wykorzystuje się protokoły losowe takie jak: ALOHA asynchroniczna, określana też mianem P ALOHA (ang. *Pure ALOHA, unslotted ALOHA*), gdzie stacje końcowe transmitują pakiety dowolnej wielkości w momencie

ich napłynięcia do bufora stacji, ALOHA synchroniczna - S ALOHA (ang. *Slotted ALOHA*), gdzie długość przesyłanych pakietów jest stała a transmisje mogą odbywać się tylko w ustalonych momentach czasu.

#### Metody dostępu rezerwacyjnego

W algorytmach dostępu korzystających z metod rezerwacji, stacja końcowa przed wysłaniem każdego pakietu (lub grupy pakietów) wysyła do stacji centralnej żądanie rezerwacji kanału satelitarnego. Po otrzymaniu przydziału kanału, transmisja pakiet lub zespół pakietów bezkolizyjnie. Zgłoszenie rezerwacji może odbywać się w przydzielonym dla każdej stacji kanale, lub w kanale wspólnym dla wszystkich stacji, zastosowaniem protokołu rywalizacyjnego (np. S-ALOHA). Tego typu protokoły określone są często mianem sztywnych algorytmów rezerwacji; w przeciwieństwie do klasy protokołów, które posiadają możliwość decydowania o tym, jaka część kanału transmisyjnego przeznaczona jest na realizację transmisji w trybie rezerwacyjnym, a jaka - na transmisję w trybie losowym; są to tzw. adaptacyjne lub dynamiczne protokoły rezerwacyjne. Jeżeli ruch jest „mały”, większa część kanału jest przeznaczana na protokół dostępu losowego. W miarę zwiększania się ruchu w sieci coraz większą część przepustowości kanału przeznacza się na protokół rezerwacyjny. Ma to wpływ na całkowite wykorzystanie kanału transmisyjnego (patrz tabela 5.4). Przykładowe protokoły tego typu to SRUC (ang. *Split Reservation Upon Collision*) oraz RAN (ang. *Random Access with Notification*).

Tabela 5.4. Przykład zmiany wykorzystania kanału dla typowego adaptacyjnego protokołu rezerwacyjnego

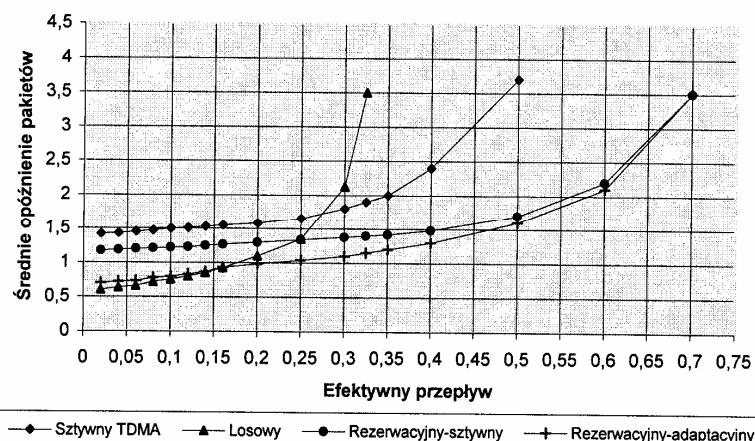
Procent kanału przeznaczony na:		Maksymalne średnie wykorzystanie kanału w [%]	Uwagi
dostęp rezerwacyjny	dostęp losowy (S-ALOHA)		
0	100	36.8	dostęp całkowicie losowy
20	80	45.4	
40	60	54.1	
50	50	58.4	
70	30	67.0	
90	10	75.7	
100	0	80.0	dostęp całkowicie rezerwacyjny

### 5.5.6.3 Metody przydziału zasobów na żądanie

W technice przydziału kanału satelitarnego na żądanie, stacje końcowe mające dane do transmisji zgłoszają zapotrzebowanie na określony „fragment” przepustowości kanału satelitarnego (pewną liczbę szczelin czasowych TDMA lub kanały częstotliwościowe FDMA na czas realizacji połączenia). Po otrzymaniu żądanego zasobów, stacje transmitują dane bezkolizyjnie. Po dokonaniu transmisji danych stacja zwraca z powrotem do wspólnej puli przydzielone jej zasoby transmisyjne. Ten system przydziału różni się od systemu z rezerwacją tym, że stacja końcowa nie musi wysyłać żądań przydziału kanału dla każdego pakietu z osobna. W przypadku mniejszej aktywności stacji końcowych dochodzi jednakże do utraty części przydzielonego stacji zasobu.

Metoda przydziału zasobów na żądanie może być stosowana zarówno w dziedzinie czasu, jako DA-TDMA (ang. *Demand Assignment TDMA*), jak też częstotliwości; nazywana jest wtedy DA-FDMA (ang. *Demand Assignment FDMA*). W sieciach VSAT, szczególnie o architekturze oczkowej, bardzo rozpowszechniony jest protokół DA-FDMA, w którym kanał satelitarny podzielony jest na pewną liczbę podkanałów z odrębnymi sygnałami nośnymi. Protokół ten jest znany pod nazwą SCPC-DAMA (ang. *Single Channel Per Carrier DAMA*) (patrz tabela 5.3).

Na rysunku 5.35 zaprezentowano zależność pomiędzy średnim opóźnieniem, a efektywnym przepływem pakietów (opóźnienie pakietów liczone jako czas upływający od momentu wygenerowania pakietu do momentu otrzymania pozytywnego potwierdzenia od adresata), dla podstawowych klas protokołów dostępu do kanału satelitarnego.



Rys. 5.35. Zależność pomiędzy średnim opóźnieniem, a efektywnym przepływem pakietów, dla podstawowych klas protokołów dostępu do kanału satelitarnego

### 5.5.7 Przyszłość sieci VSAT

Systemy satelitarne VSAT są już dojrzałą technologią, a możliwości ich dalszej ekspansji wyglądają obiecująco. Prognozy wskazują na to, że przyrost instalacji sieci VSAT ma się utrzymać w najbliższych latach na poziomie 20% rocznie. Jednakże przyszły rozwój sieci VSAT będzie zależał od tego, na ile będą one w stanie konkurować z sieciami opartymi na innych mediach transmisyjnych, np. łączach światłowodowych. Rozwój technologii VSAT powinien być ukierunkowany na zwiększenie zakresu zastosowań oraz redukcję kosztów instalacji i eksploatacji tych sieci. Duże nadzieje na dalszy rozwój systemów satelitarnych VSAT związane są z wykorzystaniem nowych pasm transmisyjnych oraz rozwojem techniki satelitarnej.

Większość działających cywilnych systemów satelitarnych (w tym sieci VSAT) wykorzystuje pasma transmisyjne o częstotliwościach poniżej 14.5 GHz. Aby zapewnić systemom satelitarnym VSAT łatwiejszą ekspansję, potrzebne są nowe pasma transmisyjne, gdyż aktualnie używane zostaną wkrótce wykorzystane. Największe zainteresowanie wiąże się z pasmem 30/20 GHz, nazywanym także pasmem Ka. Poważnym problemem w wykorzystaniu nowych pasm transmisyjnych o wysokich częstotliwościach jest ich duża wrażliwość na warunki atmosferyczne. Analitycy prognozują jednakże, że w roku 2010 liczba stacji VSAT operujących w paśmie Ka będzie wynosiła 200 000, natomiast w paśmie Ku przewidują 250 000 stacji. Duże nadzieje na rozwój sieci satelitarnych VSAT wiążą się też z nowymi typami satelitów wprowadzanych na orbitę. Satelity wielowiązkowe pozwolą na tworzenie sieci ze stacjami końcowymi wyposażonymi w bardzo małe anteny nadawczo-odbiorcze. Satelity z przetwarzaniem na pokładzie (ang. *On-Board Processing Satellites*) powinny ułatwić tworzenie sieci VSAT o architekturze oczkowej (satelita będzie pełnił rolę stacji centralnej). Ponadto wykorzystanie satelitów niskoorbitowych LEO pozwoli stworzyć sieci VSAT gwarantujące bardzo małe opóźnienia w transmisji sygnałów.

## 6 Standardy dla rozległych sieci pakietowych: X.25 i Frame Relay

Standardy X.25 i Frame Relay (wraz z ATM), opracowane dla potrzeb sieci rozległych WAN, należą do grupy technologii opartych na koncepcji przelaczania pakietów (por. rozdz. 1.2). Podstawowe różnice pomiędzy tymi standardami wynikają m.in. z odmiennego podejścia do problemu korekcji błędów, różnych wymagań nakładanych na medium transmisyjne oraz nieco innych długości jednostkowych bloków informacji przesyłanych przez sieć.

### 6.1 Protokół X.25

Już w latach siedemdziesiątych użytkownicy terminali cyfrowych, w tym komputerów, uzyskali możliwość przesyłania danych na duże odległości dzięki powstaniu tak zwanych publicznych sieci transmisji danych. W 1976 r. CCITT opracowała standard dla publicznych sieci pakietowych, znany jako zalecenie X.25. W sieciach tych jako metodę transmisji zastosowano komutację pakietów.

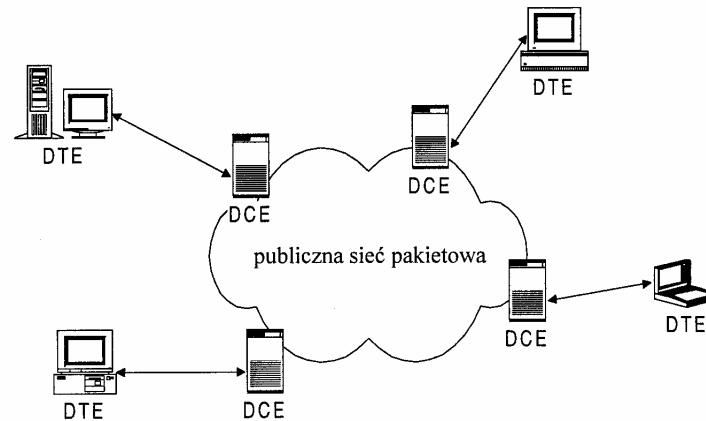
Przy ustalaniu standardu X.25 CCITT brało pod uwagę zarówno poziom rozwoju techniki komputerowej (wykorzystywany wówczas sprzęt) jak też stan techniki telekomunikacyjnej (przepustowość i niezawodność łączy telekomunikacyjnych). Znalazło to swoje odbicie w kształcie protokołów komunikacyjnych, w których istotne funkcje sieciowe zostały przypisane w znacznie większym stopniu urządzeniom sieciowym niż urządzeniom końcowym. Taki podział zadań i funkcji umożliwiał wykorzystywanie sieci X.25 do łączenia mało inteligentnych urządzeń końcowych, stanowiących w tamtym okresie większość użytkowanego sprzętu. Sieci te były budowane w oparciu o stosunkowo wolne łącza transmisyjne, o niezbyt wysokiej jakości.

Standard X.25 normalizuje zasady współpracy pomiędzy urządzeniami definiowanymi jak DTE i DCE gdzie :

**DTE** (ang. *Data Terminal Equipment*) to urządzenie końcowe transmisji danych, czyli urządzenie należące do abonenta sieci, np. terminal komputerowy, a

**DCE** (ang. *Data Communication Equipment*) stanowi węzeł sieci, czyli urządzenie komunikacyjne transmisji danych należące do przedsiębiorstwa będącego właścicielem sieci.

Strukturę sieci, zgodną z standardem CCITT X.25 ilustruje rysunek 6.1.



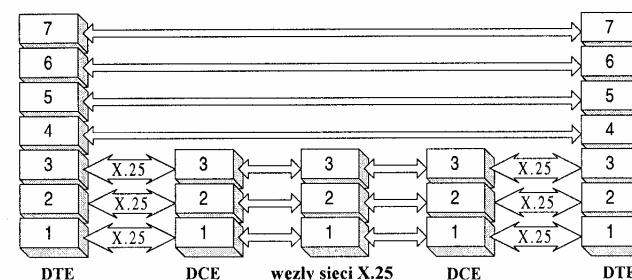
Rys. 6.1. Struktura sieci z punktu widzenia standardu X.25

#### 6.1.1 Warstwowa architektura X.25

W ramach zalecenia CCITT X.25 zdefiniowano trzy warstwy, które można uznać za realizację trzech najniższych warstw modelu ISO/OSI. Są to:

1. warstwa fizyczna,
2. warstwa łącza danych,
3. warstwa sieciowa.

Protokoły warstw wyższych (powyżej warstwy sieciowej) oraz protokoły wewnętrznsieciowe, organizujące wymianę informacji pomiędzy węzłami sieci (patrz rysunek 6.2), nie są objęte standardem X.25.



Rys. 6.2. Obszar „zainteresowany” standardu X.25

Funkcje realizowane przez poszczególne warstwy standardu X.25 są analogiczne do wypełnianych w modelu ISO/OSI.

**Warstwa fizyczna (WF)** zapewnia fizyczne połączenie pomiędzy DTE i DCE. Zalecenie CCITT X.25 pozwala użytkownikowi na wybór jednego z kilku standardów WF. W Europie najczęściej wykorzystywany jest standard X.21, który jest bardzo podobny do EIA-422. Z kolei standard X.21 bis, korzystający z interfejsu V.24/V.28, jest zbliżony do EIA-232-D. Większość publicznych sieci pakietowych w Stanach Zjednoczonych wykorzystuje standard EIA-232-D lub wcześniejszy RS-232-C jako interfejs warstwy fizycznej. Trzecim najbardziej popularnym po obu stronach oceanu rozwiązaniem WF jest standard V.35. Umożliwia on transmisję danych z szybkością 48 kb/s w Europie i 56 kb/s w USA.

**Warstwa łączą danych (WLD)** umożliwia utworzenie niezawodnego kanału logicznego w oparciu o zawodny kanał fizyczny. Warstwa łączą danych X.25 realizuje:

- kontrolę błędów,
- sterowanie przepływem danych,
- numerowanie ramek, zgodnie z mechanizmem okienkowym,
- prowadzenie statystyk wszystkich typów ruchu.

Zalecenie CCITT X.25 przewiduje zastosowanie protokołu LAP, a zwłaszcza użycie zrównoważonej procedury dostępu *Link Access Procedure Balanced* (LAPB), jako protokołu warstwy łączą danych. Warto tu nadmienić, że użycie słowa "zrównoważony" (ang. *balanced*) oznacza, że w protokole LAPB kontrola nad łączem jest w równym stopniu realizowana przez urządzenia DTE i DCE (obie strony mogą więc inicjować proces tworzenia i rozłączania połączenia).

**Warstwa sieciowa**, leżąca najwyższej w hierarchii protokołów definiowanych przez standard X.25, zapewnia łączność pomiędzy dwiema stacjami końcowymi podłączonymi do publicznej sieci pakietowej.

Protokół pakietowy PLP (ang. *Packet Layer Protocol*) warstwy sieciowej standardu X.25 realizuje szereg ważnych funkcji, w tym:

- dokonuje wyboru trasy przesyłania pakietów przez podsieć komunikacyjną,
- przeciwdziała przeciążeniom sieci, w tym powstaniu zakleszczeń w węzłach sieci,
- odpowiada, w przypadku wzajemnej współpracy sieci komputerowych, za "przeźroczysty" przekaz informacji między sieciami, dokonując w szczególności segmentacji i resegmentacji przesyłanych pakietów, a także
- definiuje formaty pakietów (ok. 30 różnych pakietów wykorzystywanych zarówno do przesyłania danych jak i obsługi ruchu służbowego), które będą przesyłane przez publiczną sieć pakietową z jednego DTE do drugiego.

Protokół warstwy 3 standardu X.25 wraz z protokołem IP, wchodzącym w skład protokołów serii TCP/IP (wykorzystywanej w globalnej sieci Internet) i IPX (preferowanym do niedawna w sieciach Novell) należy obecnie do najczęściej używanych protokołów warstwy sieciowej. Krótkie porównanie tych trzech protokołów zawarte jest w tabeli 6.1.

Tabela 6.1. Porównanie protokołów warstwy sieciowej X.25, IP i IPX

	X.25	IP	IPX
typ transmisji	połączniowa	bezołączniowa	bezołączniowa
maksymalna długość pakietu [w bajtach]	4096	64 k	546
długość nagłówka [w bajtach]	3 (pakiet informacyjny)	min. 20	30
droga pakietów przez sieć	każdy pakiet przenoszony jest przez ustalone przy zestawianiu połączenia łącze wirtualne; w każdym pakiecie zapisany jest numer łącza wirtualnego	pakiety mogą pokonywać sieć różnymi drogami; mogą być powielane, gubione, oraz dochodzić do adresata w innej kolejności niż zostały nadane; każdy pakiet przenosi adres odbiorcy - wykorzystywany przy wyznaczaniu kolejnych węzłów na trasie do węzła docelowego	podobnie jak w IP
usuwanie "bezdomnych" pakietów	nie ma potrzeby	redukcja zawartości odpowiedniego pola pakietu przy każdym przejściu przez węzeł; po osiągnięciu wartości 0 pakiet jest usuwany z sieci	podobnie jak w IP - różnica polega na tym, że zawartość odpowiedniego pola jest zwiększana
stosowanie sumy kontrolnej CRC	w warstwie niższej -2	tylko dla nagłówka; pozwala wykryć i skorygować 1 błąd	dla całego pakietu

Jak już wspomniano, rozwiązania przyjęte w X.25 dla warstw WF i WLD zostały „zapożyczone” z innych standardów, stąd w niniejszym rozdziale naszą uwagę skupimy jedynie na warstwie sieciowej standardu X.25.

### 6.1.2 Łącze wirtualne i kanał logiczny

Zadaniem warstwy sieciowej, zgodnie z zaleceniem X.25, jest sprawowanie kontroli nad tak zwanym *łączem wirtualnym* (ang. *Virtual Circuit*). Tego typu łączem zapewniają logiczne połączenie między nadawcą i odbiorcą (DTE - DTE). Aby lepiej zrozumieć znaczenie pojęcia łączem wirtualnym, należy przybliżyć inny termin wprowadzony w warstwie sieciowej - *kanał logiczny*. Warstwa 3 wykorzystuje dostarczane przez warstwę WLD łącze danych, dzieląc je na tzw. kanały logiczne. Numer takiego kanału jest przenoszony w nagłówku każdego pakietu przesyłanego przez sieć. Z każdym odcinkiem w sieci X.25 (węzeł-węzeł lub

węzeł-abonent końcowy) związana jest określona liczba kanałów logicznych. Jest to maksymalna liczba równocześnie prowadzonych sesji transmisyjnych na danym odcinku. Protokół pozwala na utworzenie maksymalnie do 4095 kanałów logicznych.

Liczba kanałów logicznych wiąże się przy tym z maksymalną przepustowością uzyskiwaną w pojedynczym kanale oraz charakterystyką ruchu generowanego przez DTE. Dla przykładu - jeżeli abonent wykorzystuje swoje łączne dla dużej liczby połączeń wymagających małej przepustowości (terminal tekstowy), to sensownym jest wtedy podział łącza na wiele kanałów logicznych.

Łącze wirtualne składa się z wszystkich kanałów logicznych, które są wykorzystywane do realizacji połączenia między dwiema stacjami końcowymi DTE.

Istnieją dwa rodzaje połączeń między oddalonymi DTE (analogicznie do sieci telefonicznej). Są to:

- **Łącze stałe PVC** (ang. *Permanent Virtual Circuit*), które nie wymaga zestawiania i usuwania połączenia (analogicznie do łączów dzierżawionych). Łącze wirtualne składa się wówczas z przydzielonych na stałe kanałów logicznych. Transmisja odbywa się wg. identycznych zasad, jak dla łącz przełączanych.
- **Łącze przełączane VC** (ang. *Virtual Call*), wymagające każdorazowego zestawiania na czas połączenia (podobnie do komutowanych łącz telefonicznych).

### 6.1.3 Jednostki danych w X.25

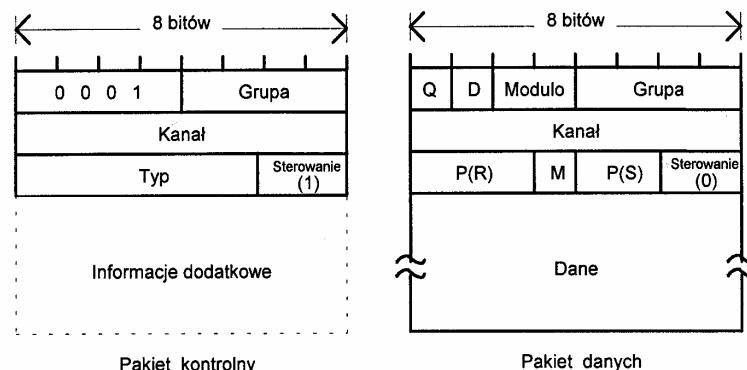
Protokół każdej warstwy modelu odniesienia OSI definiuje swoją jednostkę danych PDU (ang. *Protocol Data Unit*). Jedną z idei tego modelu jest to, iż warstwa niższa nie ingeruje we wnętrzu jednostki danych warstwy wyższej, a tylko dodaje do niej informacje, które umożliwiają wykonywanie powierzonych jej zadań i funkcji.

Zalecenie CCITT X.25 opisuje protokoły i jednostki danych trzech najniższych warstw modelu odniesienia OSI. Jednostką danych protokołu sieciowego jest pakiet (stąd bierze się często używana nazwa warstwy trzeciej - warstwa pakietowa). Możemy przy tym wyróżnić trzy grupy pakietów:

1. Pakiety wykorzystywane przy zestawianiu i kasowaniu połączeń oraz restarcie (reinicjowaniu) już istniejących połączeń.
2. Pakiety przenoszące dane użytkownika.
3. Pakiety nadzorcze, za pomocą których realizowana jest kontrola przepływu na poziomie warstwy sieciowej.

Zaprezentowana powyżej klasyfikacja pakietów ma na celu zwrócenie uwagi na wiele analogii między przedstawionymi pakietami, a ramkami używanymi w warstwie łącza danych.

Na rysunku 6.3 przedstawiono postać pakietów standardu X.25 (rysunek 6.3a - pakiety kontrolne i rysunek 6.3b - pakiety danych).



Rys. 6.3. Formaty pakietów w X.25

Pakiety danych składają się z nagłówka i danych użytkownika. Dane użytkownika są przekazywane do warstwy sieciowej z warstw wyższych. Dodanie nagłówka umożliwia m.in. identyfikację pakietów oraz adresowanie.

Pakiety kontrolne nie zawierają danych z warstw wyższych i są wykorzystywane do realizacji ruchu służbowego warstwy sieciowej (tworzenie i rozłączanie łącz wirtualnych, itp.).

### 6.1.4 Procedury komunikacyjne w X.25

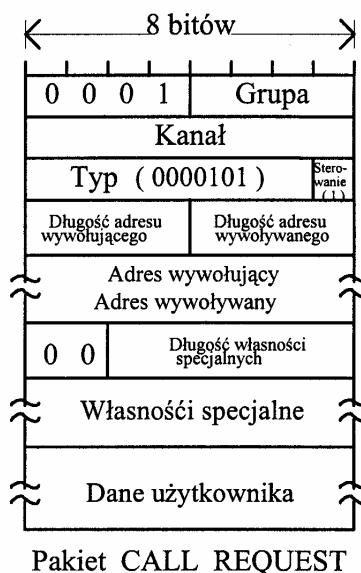
Dla potrzeb X.25 opracowano szereg procedur komunikacyjnych. Poniżej przedstawujemy krótkie charakterystyki poszczególnych procedur, koncentrując się na zasygnalizowaniu funkcji realizowanych przez standardowe pakiety wykorzystywane w różnych fazach realizacji połączenia.

#### 6.1.4.1 Zestawianie, kasowanie (likwidacja) i restartowanie połączeń

Do zestawiania połączenia, jego kasowania i restartu używane są standardowe pakiety CALL REQUEST, CALL ACCEPTED, CLEAR REQUEST, CLEAR CONFIRMATION, RESET REQUEST, RESET CONFIRMATION oraz DIAGNOSTIC.

**CALL REQUEST** - pakiet ten wysyłany jest przez zainteresowane DTE; dociera on do odległego DTE (adresata) jako INCOMING. Postać pakietu CALL REQUEST ilustruje rysunek 6.4.

**CALL ACCEPTED** - akceptacja wywołania CALL REQUEST, innymi słowy - zgoda na nawiązanie połączenia. Pakiet ten dochodzi do DTE, będącego inicjatorem połączenia jako CALL CONNECTED.



Rys. 6.4. Przykład pakietu kontrolnego i znaczenia zawartości pola Typ w zależności od rodzaju pakietu

**CLEAR REQUEST** - żądanie rozłączenia; pakiet ten jest wysyłany przez DTE, gdy wszystkie dane użytkownika zostały poprawnie nadane. Do DTE - partnera pakiet ten dochodzi jako CLEAR INDICATION (sygnalizując potrzebę rozłączenia). Również DCE może wykorzystać ten pakiet w przypadku, gdy połączenie nie może być utrzymane ze względu na np. problemy techniczne. W takim przypadku oba DTE otrzymują „od sieci” pakiet CLEAR INDICATION. Pakiety CLEAR REQUEST są automatycznie generowane przez sieć, jeżeli pakiety CALL REQUEST nie mogą być przesłane. W takich przypadkach zapisywana jest w nich przyczyna rozłączenia. Typowymi przyczynami są: zajętość numeru lub przeciążenie sieci.

**CLEAR CONFIRMATION** - akceptacja skasowania połączenia; pakiet ten wysyłany jest przez DTE - partnera stacji inicjującej proces rozłączenia. Pakiet ten w drodze przez sieć nie zmienia swojego statusu (nazwy) i dochodzi do stacji "żądającej" rozłączenia (DTE lub DCE) jako CLEAR CONFIRMATION.

**RESET REQUEST** - żądanie resetowania-zerowania połączenia; pakiet używany przy wychodzeniu z różnych sytuacji nieprawidłowych np. stanu powstałego w wyniku wykrycia pakietu danych z błędnym numerem. Może być wysyłany przez DTE i DCE. Do adresata dochodzi jako RESET INDICATION. Resetowanie

połączenia sprowadza się do wyzerowania liczników pakietów danych (będących tzw. zmiennymi stanu kanału).

**RESET CONFIRMATION** - akceptacja przeprowadzenia zerowania łącza; jest odpowiedzią na pakiet RESET INDICATION i w drodze przez sieć nie zmienia swojej nazwy.

**RESTART REQUEST** - żądanie zainicjowania styku DTE/DCE; inicjalizacja styku następuje po zgłoszeniu przez warstwę 2 ustanowienia połączenia. Pakiet ten ma zawsze charakter lokalny DTE-DCE. Do adresata dochodzi jako RESTART INDICATION. Przyczyną wysłania go w czasie trwania połączenia jest najczęściej poważniejsze uszkodzenie DTE bądź DCE. W takim wypadku wszystkie korzystające z tego kanału logicznego stacje pracujące w trybie VC zostaną poinformowane o rozłączeniu (wysłanie pakietów RESET REQUEST), a pracujące w trybie PVC - o zerowaniu połączenia.

**RESTART CONFIRMATION** - zezwolenie na restart; pozytywna odpowiedź na pakiet RESTART REQUEST.

**DIAGNOSTIC** - pakiet diagnostyczny; używany w niektórych sieciach do wychodzenia z sytuacji błędnych, z których wyjście nie jest możliwe przy użyciu standardowych metod (RESET, RESTART).

#### 6.1.4.2 Transmisja danych użytkownika

W fazie przekazu danych wymieniane są głównie pakiety DATA.

**DATA** - pakiet z danymi użytkownika (warstwy 4 - transportowej); wysyłany przez DTE. Format tego pakietu ilustruje rysunek 6.3.

**INTERRUPT** - specjalny pakiet pozwalający na nadawanie poza kolejnością krótkich jednobajtowych sygnałów. Ze względu na to, że pakiety te nie mają numerów sekwencyjnych, mogą być dostarczane natychmiast po ich nadejściu (omijając kontrolę przepływu), bez względu na to, ile kolejnych pakietów znajduje się przed nimi w kolejce. Pakiet INTERRUPT potwierdzany jest za pomocą pakietu INTERRUPT CONFIRMATION. Typowym jego zastosowaniem jest przesyłanie znaku przerwania (np. ESC) od terminala.

#### 6.1.4.3 Kontrola przepływu danych

Funkcje wymienionych poniżej pakietów są identyczne jak analogicznych ramek używanych do kontroli przepływu w warstwie łącza danych. (patrz paragraf 3.5.9 - protokół LAPB).

**RECEIVE READY (RR)** - potwierdzenie pakietu danych i zgłoszenie stanu gotowości.

**RECEIVE NOT READY (RNR)** - potwierdzenie pakietu danych oraz żądanie zatrzymania transmisji - stacja nie jest w stanie przyjmować kolejnych pakietów.

**REJECT (REJ)** - żądanie retransmisji grupy pakietów (począwszy od numeru zawartego w polu pakietu REJ).

Znaczenie pól tego pakietu jest następujące:

**GRUPA** i **KANAŁ** razem tworzą 12-bitowy numer łącza wirtualnego; DTE może mieć jednocześnie do 4095 łącz wirtualnych (numer zerowy jest zarezerwowany).

**TYP** - identyfikacja pakietu.

**STEROWANIE** - 1 - dla pakietów kontrolnych i 0 - dla pakietów z danymi; umożliwia to DTE bardzo szybkie określenie czy nadchodzący pakiet zawiera dane, czy informacje sterujące.

**Q** - bit umożliwiający kwalifikację danych przez warstwy wyższe.

**P(S)** - pole wykorzystywane do zapisywania numerów sekwencyjnych pakietów.

**P(R)** - pole używane przy przesyłaniu potwierdzeń; umieszcza się w nim numer pakietu następnego po ostatnio poprawnie odebranym.

**Modulo** - dwa bity określające zakres używanych numerów sekwencyjnych. Możliwe wartości: 10 - numeracja na 3 bitach <0,7>,

01 - numeracja na 7 bitach <0,127>. Wartości 00 i 11 są niezdefiniowane i można je wykorzystać do przesłania innej informacji.

**D** - bit określający znaczenie odbieranych potwierdzeń. Dla D=0 nadchodzące potwierdzenie oznacza tylko to, że pakiet został odebrany poprawnie przez lokalne DCE, nie oznacza jednak, że oddalone DTE odebrało ten pakiet.

Gdy D=1, potwierdzenie jest "prawdziwym" potwierdzeniem między końcowymi komunikującymi się stacjami (DTE).

**M (More)** - bit wykorzystywany przez DTE do oddzielania grup pakietów przenoszących jedną wiadomość. Wysłanie długiej wiadomości sprowadza się do ustawiania bitu M=1 we wszystkich pakietach z wyjątkiem ostatniego. Takie postępowanie uniemożliwia węzłom sieci upakowanie w jeden pakiet danych pochodzących z różnych wiadomości (w przypadku segmentacji w węzłach pośrednich).

**DANE** - pole przeznaczone do przenoszenia danych użytkownika (warstwy transportowej) jest równa 2. Standardowa długość tego pola wynosi 128 bajtów, jednak istnieje możliwość negocjacji innej długości: 16, 32, 64, 256, 512, 1024, 4096 bajty.

#### 6.1.4.4 Sterowanie przepływem

Sterowanie przepływem w warstwie 3 odbywa się przy użyciu tej samej techniki, co w warstwie 2. Wykorzystywany jest mechanizm przesuwnego okna, a dokładniej protokół "Go Back N".

Standardowa szerokość okna nadawczego (określająca liczbę pakietów jakie mogą być wysłane bez konieczności oczekiwania na potwierdzenie najwcześniej szerszego z nich). Dopuszczalne wartości okna W mieszczą się w przedziale od 1

do MaxSeq (maksymalny numer sekwencyjny). Szerokość okna odbiorczego jest stała i wynosi 1.

Typowa jest też numeracja pakietów: standardowa w zakresie 0 - 7 (3 - bity) i rozszerzona 0 - 127 (7 - bitów). Numery sekwencyjne ramek zawierających dane zapisywane są na polu P(s).

Potwierdzanie poprawnego odbioru pakietów możliwe jest poprzez wysyłanie tzw. potwierdzeń wtrąconych (ang. *piggybacking*), czyli umieszczanie numeru kolejnego pakietu po ostatnio poprawnie odebranym w polu P(r) pakietu "Dane". W przypadku braku ruchu zwrotnego wykorzystywane są pakiety kontrolne RR, REJ, RNR.

#### 6.1.4.5 Adresowanie

Adresowanie dotyczy tylko łącz przełączanych (VC). Umożliwia ono identyfikację odpowiednich DTE. W polach adresowych pakietów CALL REQUEST i CALL ACCEPTED umieszcza się zakodowane w kodzie BCD (ang. *Binary Coded Decimal* - każda cyfra dziesiętna zapisywana jest na 4- bitach) cyfry dziesiętne.

Pierwsze cztery cyfry określane jako DNIC (ang. *Data Network Identification Code*) służą do identyfikacji sieci. Przykładowo, polskie sieci pakietowe mają numery rozpoczynające się od 260: TELBANK DNIC=2603, PKONET DNIC=2605. Pozostałe cyfry z pola adresowego (z reguły 10 cyfr) określają numer terminala (DTE) w konkretnej sieci.

#### 6.1.4.6 Udogodnienia

Protokół X.25 umożliwia elastyczne dostosowywanie się do potrzeb abonentów, proponując im możliwość zmiany poszczególnych parametrów połączenia. Mechanizm ten określany jako "udogodnienia" (ang. *facilities*) wykorzystuje pole "Właściwości specjalne" pakietów CALL REQUEST i CALL ACCEPTED. Składa się ono z 8-bitowego pola będącego kodem danego udogodnienia i opcjonalnie pola przeznaczonego na parametr.

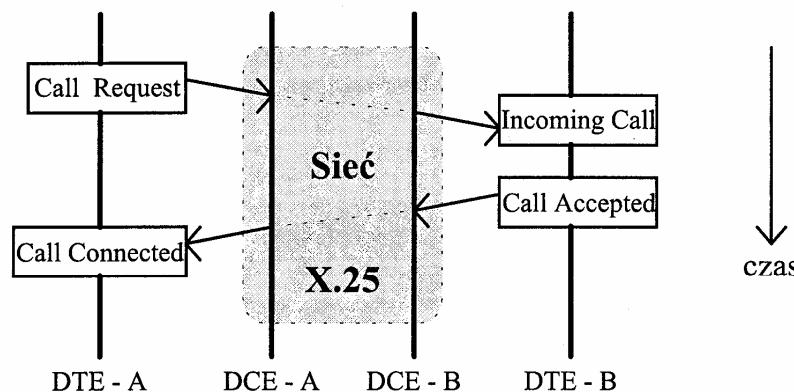
Przykłady typowych udogodnień to:

- różne przepustowości dla obu kierunków transmisji,
- zmiana długości pakietów,
- zmiana szerokości okna nadawczego,
- możliwość realizacji połączenia na koszt odbiorcy.

#### 6.1.4.7 Przebieg połączenia w X.25

##### Zestawianie połączenia

Schematyczny przebieg zestawiania połączenia w sieciach pakietowych, działających zgodnie z protokołem X.25, pokazany jest na rysunku 6.5.



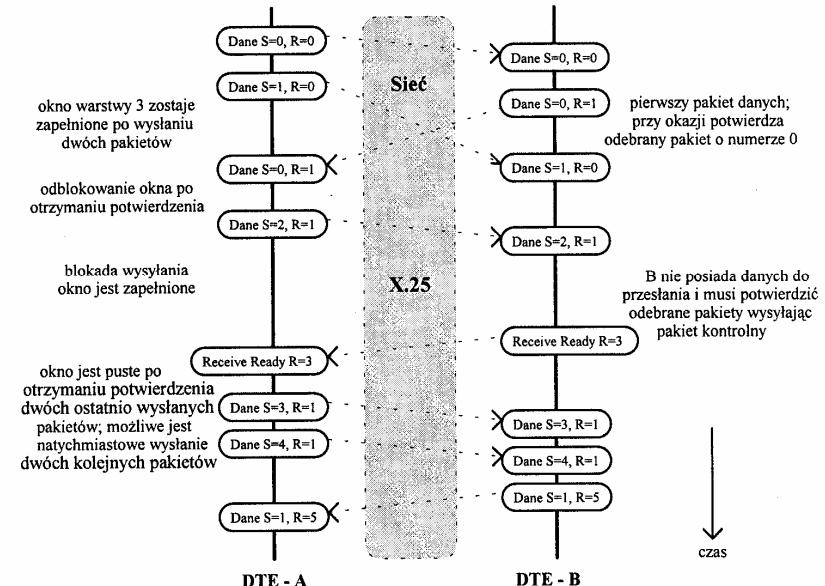
Rys. 6.5. Nawiązanie połączenia między dwoma DTE

Podejmowane kolejno działania są następujące:

1. DTE wywołujące, oznaczane dalej jako A, wysyła do swojego lokalnego DCE (odpowiednie DCE oznaczone będą dalej jako DCE-A i DCE-B) pakiet CALL REQUEST w wybranym przez siebie wolnym kanale logicznym. Numer tego kanału zapisuje w polu KANAŁ. Wszystkie przychodzące i wychodzące pakiety, w trakcie tego połączenia, będą identyfikowane za pomocą tego numeru.
2. Sieć przenosi pakiet CALL REQUEST do DCE-B.
3. DCE-B odbiera pakiet CALL REQUEST i przesyła go jako INCOMING CALL do B (DTE - wywoływanie). Pakiet ten ma ten sam format co CALL REQUEST z wyjątkiem numeru kanału logicznego, który jest wybierany przez DCE-B spośród aktualnie wolnych kanałów.
4. B wyraża zgodę na nawiązanie połączenia przez wysłanie pakietu CALL ACCEPTED z numerem kanału identycznym jak w pakiecie INCOMING CALL.
5. A odbiera pakiet CALL CONNECTED, z tym samym numerem kanału co w wysłanym przez siebie pakiecie CALL REQUEST, i w tym momencie A i B mogą rozpoczęć wymianę danych.

#### Transmisja danych

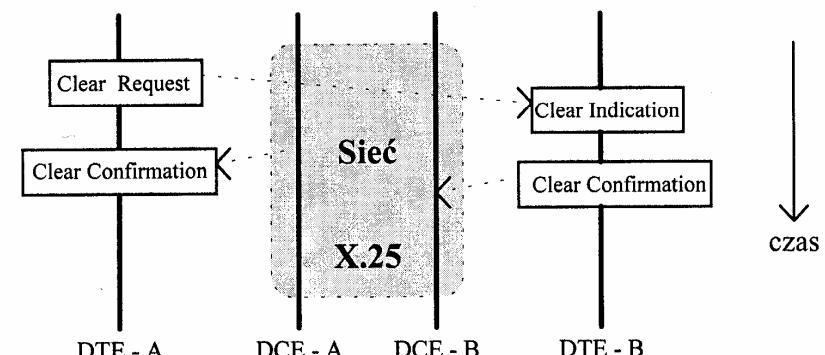
Przykładowy przebieg transmisji danych pokazuje rysunek 6.6. Warto zauważyć, że większość potwierdzeń przesyłana jest jako „wtrącone” do ruchu zwrotnego, co znacznie zwiększa efektywność pracy systemu.



Rys. 6.6. Przykładowa sekwencja zdarzeń w fazie transmisji danych wg protokołu X.25

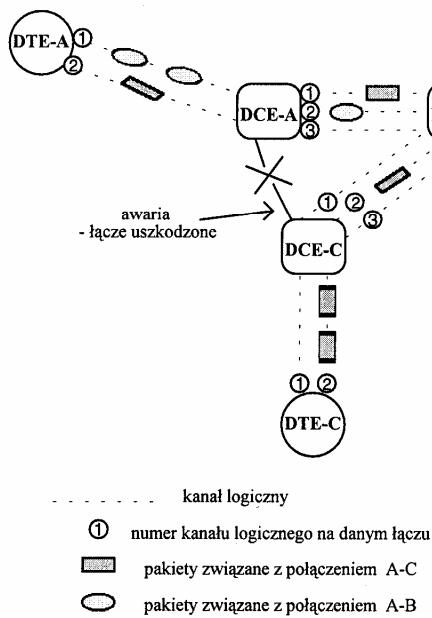
#### Rozłączanie połączenia

Każda z komunikujących się stron może rozłączyć połączenie przez wysłanie pakietu CLEAR REQUEST. Sekwencję zdarzeń związanych z procedurą rozłączania przedstawia rysunek 6.7.



Rys. 6.7. Rozłączanie łącza wirtualnego

#### 6.1.4.8 Komutacja pakietów w sieci X.25



Rys. 6.8. Przesyłanie pakietów przez łączę wirtualne w X.25

Pakiety w sieciach działających wg. standardu X.25 przesyłane są przez łączę wirtualne. Zestawianie takiego łączka odbywa się w kilku zasadniczych fazach (ilustruje to rysunek 6.8):

Faza 1. W pierwszej fazie określany jest pierwszy segment łączka wirtualnego stanowiący kanał logiczny wybrany przez DTE inicjujące połączenie (czyli DTE wysyłające pakiet Call Request wybranym przez siebie kanałem logicznym).

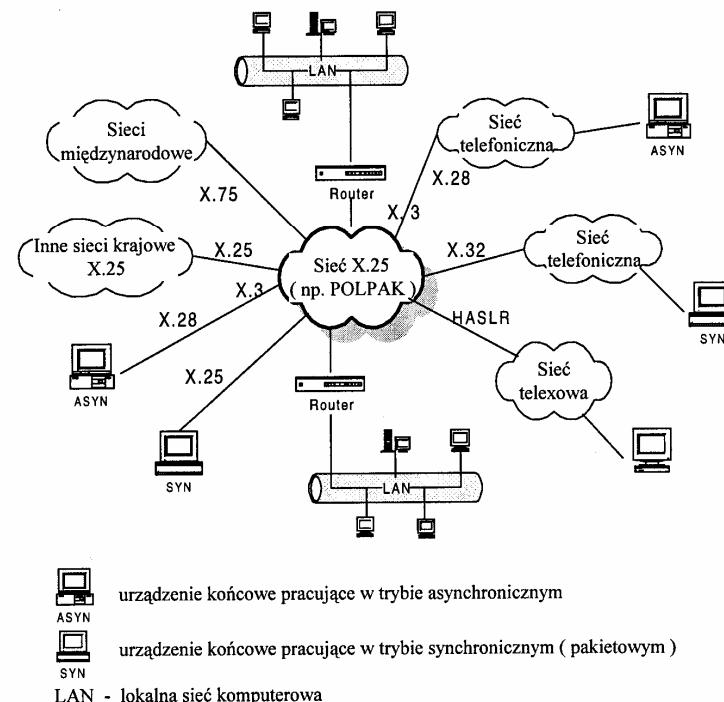
Faza 2. Lokalny węzeł (DCE) po odebraniu pakietu Call Request i odczytaniu adresu docelowego wybiera kolejny węzeł, do którego kieruje pakiet, wykorzystując posiadane informacje o obciążeniu sieci na poszczególnych kierunkach. DCE dokonuje też wyboru wolnego kanału logicznego (łączka międzwęzłowe podzielone są tak samo jak łączka DTE-DCE na kanały logiczne) i wysyła pakiet Call Request do następnego węzła.

Faza 3. Opisana powyżej procedura realizowana jest we wszystkich pośrednich węzłach, aż do momentu osiągnięcia przez pakiet docelowego DTE. Wszystkie odcinki drogi jaką przebył pakiet Call Request wraz z odpowiednimi numerami kanałów logicznych składają się na utworzone w ten sposób łączce wirtualne.

Wszystkie pozostałe pakiety związane z tym połączeniem będą przesyłane, w obu kierunkach tą samą drogą, z zachowaniem ich kolejności.

#### 6.1.4.9 Łączenie X.25 z innymi sieciami

CCITT zdefiniował też dokładnie sposoby wymiany informacji pomiędzy różnymi typami sieci. Zawarte one są w odpowiednich zaleceniaach serii X: X.32, X.28, X.75, X.3, X.29.



Rys. 6.9. Łączenie stacji końcowych i innych sieci komputerowych z siecią X.25

Rysunek 6.9 przedstawia różne sposoby dostępu do sieci pracującej zgodnie z X.25. Wykorzystując tzw. routery czyli „sprzęgi” międzsieciowe istnieje możliwość łączenia przez sieć X.25 sieci lokalnych (LAN) stosujących protokoły

sieciowe typu IP czy Novell IPX. Każdy pakiet przed wprowadzeniem do sieci X.25 jest wówczas przekształcany do postaci zgodnej z X.25, a na wyjściu z sieci jego format jest ponownie dostosowywany do postaci wymaganej przez dany protokół drugiej sieci LAN.

Na zakończenie warto dodać, że w Polsce standard X.25 wykorzystuje się w 10 (czy też jedynie 10-ciu) sieciach pakietowych (są to m.in. Polpak, Kolpak, Telbank, PKOnet, Cupak, Nask). Dla sieci pakietowych przydzielone zostały Polsce numery od 2600 do 2609.

## 6.2 Podstawy Standardu Frame Relay

Standard Frame Relay (FR) należy do stosunkowo nowych standardów opracowanych dla pakietowych sieci rozległych - WAN. Postęp technologiczny, szczególnie widoczny w ciągu ostatnich kilkunastu lat, doprowadził do zdezaktualizowania się założeń, które legły u podstaw opracowania standardu X.25. Rozwój techniki i nowoczesnych technologii VLSI spowodował gwałtowny przyrost mocy obliczeniowych komputerów. Komputery osobiste mają dziś możliwości obliczeniowe porównywalne z komputerami obliczeniowymi sprzed 15-20 lat. Z kolei rozwój technologii telekomunikacyjnych doprowadził do wdrożenia i upowszechnienia się szybkich i niezawodnych łącz o bardzo dużych przepustowościach i wysokiej jakości transmisji. W takiej sytuacji można było stosunkowo dużo zadań, realizowanych w standardzie X.25 przez urządzenia sieciowe, przenieść na urządzenia końcowe. Wyższa jakość łącz telekomunikacyjnych umożliwiła ograniczenie do zupełnego minimum ruchu sygnalizacyjnego (słужbowego) w sieci. Opierając się na takich założeniach (krańcowo odmiennych od założeń, w oparciu o które powstało zalecenie CCITT X.25) stworzono nowy standard sieci WAN znany jako Frame Relay.

Frame Relay należy do grupy technologii opartych na koncepcji komutacji pakietów (w tym przypadku przełączania ramek). Pod pojęciem pakietu rozumiemy jednostkową porcję informacji przesyłaną przez sieć. Do tej rodziny systemów należy zarówno najstarsza i najlepiej udokumentowana technologia X.25, jak i najnowsza ATM. Często w celu podkreślenia różnic, FR i ATM określa się mianem technologii szybkiego przełączania pakietów. Podstawowe różnice między X.25 a nowymi standardami Frame Relay czy ATM dotyczą m.in.:

- Podejście do problemu korekcji błędów;
- Wymagań nakładanych na medium transmisyjne;
- Długości jednostkowego bloku informacji przesyłanego przez sieć.

### 6.2.1 Standardyzacja Frame Relay

Najważniejszymi organizacjami zajmującymi się tworzeniem oficjalnych, międzynarodowych standardów w dziedzinie teleinformatyki są: CCITT (ITU-T)

i ANSI. Podstawowe dokumenty, z których wywodzi się współczesny kształt technologii FR, powstały właśnie w tych organizacjach.

Pakietowa sieć transmisyjna FR nie powstała jako samodzielna, niezależna technologia. Pierwsze opracowania zostały zawarte w grupie dokumentów definiujących standard ISDN. Dotyczyły one protokołu transmisji danych charakteryzującego się:

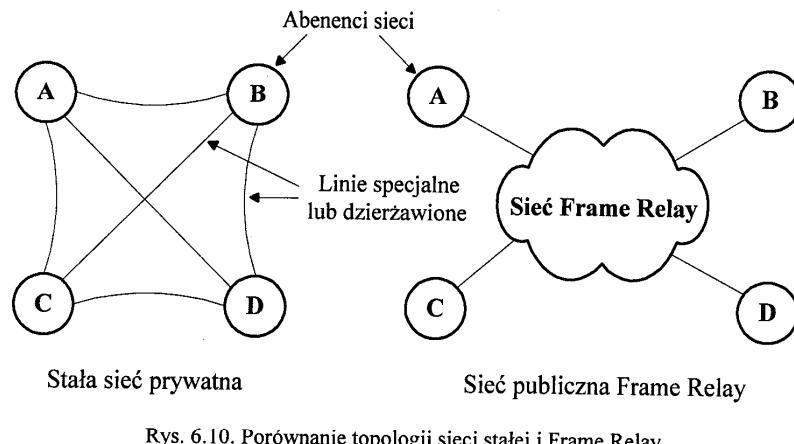
- Wysoką efektywnością;
- Ograniczonymi mechanizmami korekcji błędów;
- Niskimi opóźnieniami transmisji.

Tabela 6.2. Standardy odnoszące się do techniki przekazywania ramek Frame Relay

Parametr	ANSI	CCITT	Przedmiot normalizacji
Usługa	T1.606	I.233	Cel, zastosowanie, właściwości, parametry, możliwości, ograniczenia.
Przeciwdziałanie przeciążeniu	T1.606 Aneks	I.370	Pomiary ruchu użytkowników, przydział zasobów, technika sondażu (dostosowanie wymagań użytkowników i pojemności sieci).
Główne aspekty	T1.618	Q.922	Protokół transmisji danych użytkownika łącznie z formatem ramki i nadzorem przeciążeniowym.
Protokół łącza danych		Q.922	Procedura oparta na LAP D ( <i>Link-Access Protocol, D channel</i> ) dla łącza danych FR w sieci ISDN.
Sygnalizacja dostępu	T1.933	Q.933	Budowa, zestawienie wirtualnych połączeń w technice FR, powiadomienie o zestawieniu stałego połączenia wirtualnego PVC.
Dopasowanie	T1.612 12	V.1120	Dopasowanie części asynchronicznej HDLC do stosowania przez usługę przenoszeniową (ISDN) techniki FR.

Jednak pod wpływem presji producentów zdecydowano się na wyodrębnienie protokołu FR i stworzenie standardu, który miałby zastosowanie również poza siecią ISDN. Komitet standaryzacyjny CCITT zdefiniował w 1988 roku specyfikację I.122, w której określił zasady przesyłania pakietów w sieci FR. Zestawienie standardów dotyczących FR przedstawiono w tabeli 6.2. Sieć FR uzupełniona o mechanizm tworzenia połączeń wirtualnych staje się rozwiązaniem następującym istniejące, lecz mało efektywne, sieci z protokołem X.25. Najnowsza wersja zalecenia I.122 (1994 r.) rekomendowana przez CCITT określa sieć FR jako usługę podstawową, stosowaną w relacji użytkownik-użytkownik lub użytkownik-dowolna, inna sieć, szczególnie w zakresie transmisji danych. Korzystanie z usług FR zmniejsza czas

transportu danych przez sieć w porównaniu z protokołem X.25, oferując większą niezawodność transmisji i elastyczne wykorzystanie zasobów transportowych istniejących mediów transmisyjnych. Powoduje to coraz szerszą implementację tej technologii w sieciach pakietowych PSPDN (ang. *Public Switched Packet Data Network*), zastępując specjalne i dzierżawione linie transmisyjne (rys. 6.10).



Rys. 6.10. Porównanie topologii sieci stałej i Frame Relay

### 6.2.2 Frame Relay Forum

Dokumenty standaryzacyjne określiły ramy protokołu FR, pozostało jednak wiele zagadnień szczegółowych, wymagających dodatkowych regulacji. Firmy zajmujące się konstrukcją urządzeń sieciowych i upowszechnianiem technologii FR postanowiły przyspieszyć proces standaryzacji. Podjęły aktywne działania mające na celu stworzenie organizacji, zadaniem której byłoby kreowanie i rozpowszechnianie rozwiązań technicznych. W ten sposób pewne zalecenia stawałyby się "de facto" standardami jeszcze przed ich oficjalnym zatwierdzeniem przez komitety CCITT i ANSI. Założycielami i inicjatorami całej akcji były cztery firmy: Digital Equipment Corporation (DEC), Northern Telecom, Cisco, Stratacom.

Pierwszym krokiem "grupy czterech" - taką bowiem nazwę przyjęła organizacja - było opracowanie, na podstawie zaleceń komitetu ANSI i CCITT, dokumentu zawierającego istotne rozszerzenia specyfikacji FR. Ułatwiło to współpracę między urządzeniami i zapewniło zgodność na poziomie protokołu. Inne firmy, korzystając z wprowadzonych rozszerzeń, zaczęły dostosowywać swoje urządzenia i programy, akceptując podane zalecenia "grupy czterech". Z powodu rosnącej liczby korporacji, pragnących korzystać z powstających rekomendacji, a także mieć wpływ na ich przyszły kształt, zdecydowano się na utworzenie Frame Relay Forum.

### 6.2.3 Frame Relay jako jedna z technologii przełączania pakietów

Powszechnie akceptowanym standardem dotyczącym transmisji danych w pakietowej sieci publicznej jest X.25. Kluczowe cechy tego zalecenia:

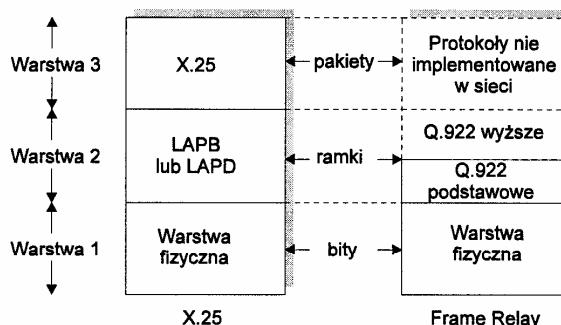
- Przesyłanie pakietów kontrolnych połączenia (używane do zestawiania i rozłączania kanałów wirtualnych) jak i przesyłanie pakietów danych odbywa się tym samym kanałem, w efekcie czego, używana jest sygnaлизacja wewnętrz pasma;
- Multipleksowanie kanałów wirtualnych odbywa się w warstwie 3-ciej;
- Zarówno warstwa 3-cia jak i 2-ga zawierają mechanizmy sterowania strumieniem danych i kontroli błędów.

Ponieważ w czasie tworzenia standardu X.25 poziom techniki teletransmisyjnej, a także jakość fizycznego medium narzucały stosunkowo wysoką stopę błędów przy transmisji danych, więc wymagało to stworzenia wewnętrz protokołu komunikacyjnego mechanizmów korekcji i retransmisji pakietów. Komunikacja między użytkownikami odbywała się w X.25 na zasadach nawiązywania połączenia i zestawiania sesji, podczas której wymieniane były informacje. Niezawodność transmisji gwarantowano za pomocą mechanizmu potwierdzeń dokonywanych między kolejnymi węzłami. Wraz z upływem czasu standard X.25 - z uwagi na przystosowanie do pracy na wolnych łączach i z uwagi na dużą liczbę danych informacyjnych - okazał się niewystarczający.

*FR w swoich generalnych założeniach jest podobne do X.25. Zakłada zmienną długość ramek oraz tworzenie połączeń logicznych, czyli tzw. kanałów wirtualnych i podobnie jak X.25 definiuje styk między użytkownikiem, a siecią, na zasadach DTE/DCE.* Na tych jednak kończą się wzajemne podobieństwa. Specyfikacja FR definiuje styk użytkownika z urządzeniami sieciowymi z wykorzystaniem dwóch pierwszych warstw modelu ISO-OSI. Użytkową jednostką informacji stosowaną w sieci FR jest rama. U podstaw wyodrębnienia protokołu Frame Relay ze zbioru standardów ISDN było założenie, iż będzie on miał zastosowanie na szybkich łączach o niskiej stopie błędów. W związku z tym, zrezygnowano zupełnie z mechanizmów korekcji i retransmisji na poziomie protokołu sieciowego. Te zadania pozostały wyższym, "inteligentnym" warstwom modelu ISO-OSI, które muszą być implementowane w urządzeniach końcowych. Dzięki temu proces wyboru drogi, którą wędrują ramki, został przeniesiony na poziom warstwy drugiej. Pozwoliło to uzyskać minimalne czasy przełączania w węzłach sieci i zapewnia szybkość transmisji co najmniej 2 Mb/s.

*FR został zaprojektowany w celu ograniczenia kosztów związanych z funkcjonowaniem pakietowych sieci publicznych opartych na standardzie X.25.* Porównanie stosów protokołów X.25 i FR przedstawiono na rysunku 6.11. Różnice pomiędzy FR, a konwencjonalną usługą komutacji pakietów X.25 można przedstawić następująco:

- Sygnalizacja dotycząca kontroli wywołania przenoszona jest wydzielonym kanałem logicznym, innym niż dane użytkownika. Tak więc, węzły pośrednie nie muszą stosować indywidualnego połączenia w celu utrzymywania tablic stanów lub przetwarzania komunikatów kontroli wywołania;
- Multiplexowanie i komutacja połączeń logicznych ma miejsce w warstwie 2-giej, a nie w 3-ciej. W ten sposób całkowicie wyeliminowano jedną warstwę w procesie przetwarzania;
- Sterowanie przepływem danych i kontrola błędów nie odbywają się na każdym etapie transmisji. Za sterowanie przepływem danych typu end-to-end i kontrolę błędów są odpowiedzialne warstwy wyższe, jeśli wszystkie są wykorzystywane.



Rys. 6.11. Porównanie stosów protokołów X.25 i Frame Relay

Technologia przełączania ramek Frame Relay wypiera eksploatowane dotychczas sieci pakietowe X.25. W stosunku do tych sieci, sieci FR wykazują szereg istotnych zalet takich, jak:

- Redukcja opóźnienia komutacji do 2 ms;
- Zwiększenie przepływności w łączach nawet do 45 Mb/s;
- Możliwość współpracy z sieciami LAN i ATM;
- Zapewnienie połączeń wirtualnych w prywatnych sieciach komunikacyjnych.

#### 6.2.4 Zastosowanie sieci FR

Oferta technologii FR jest dostosowana do różnych szybkości linii transmisyjnych, a w szczególności: 56 kb/s, 64 kb/s, 256 kb/s, 768 kb/s, 1544 kb/s, 2,048 Mb/s, a nawet 45 Mb/s - co w porównaniu ze standardem X.25 (1200 b/s - 64 kb/s) powiększa znacznie zakres zastosowań sieci. Podstawowe kierunki zastosowań obejmują:

- Łączenie różnego typu odległych sieci LAN przez mosty, routery i multipleksery;

- Przesyłanie dużych plików danych między stacjami roboczymi np. o wysokiej rozdzielcości CAD/CAM, a komputerową bazą danych przez rozległe sieci WAN. Dzięki FR możliwa jest np. transmisja plików wymagających małych opóźnień i dużych przepływności;
- Pracę interaktywną między terminalami użytkowników o niewielkim ruchu a zasobami dużego komputera, zwykle z wykorzystaniem multipleksera statystycznego agregującego komunikaty napływające od wielu użytkowników;
- Komunikację interaktywną wymagającą krótkich komunikatów z małymi opóźnieniami przy niewielkiej przepływności ruchu.

Sieć z przełączaniem ramek nie jest jednak odpowiednia dla przesyłania głosu lub wolnozmiennych danych wymagających przetwarzania w czasie rzeczywistym. Technologia szybkiego przełączania ramek FR (podobnie jak przełączanie pojedynczych komórek w ATM) jest szczególnie przydatna w zastosowaniach związanych z sieciami B-ISDN, a więc tam, gdzie w środowisku transmisyjnym występują nieprzewidywalne nasilenia ruchu lub okresowy wzrost aktywności. Stany te są charakterystyczne dla sieci LAN, w których natężenie ruchu wzrasta w określonych porach dnia, lub dla usług e-mailowych potrzebujących okresowego wzrostu przepływności sieci.

#### 6.2.5 Ewolucja w kierunku ATM

Rosnąca liczba użytkowników postrzega przekaz ramek FR jako technikę przejściową, prowadzącą do ATM. Większość z nich planuje przeniesienie przez sieci ATM ruchu związanego z przekazem ramek FR i bezpołączeniową transmisję danych SMDS (ang. *Switched Multi-Megabit Data Service*).

Z myślą o rozwoju FR zakłada się, że sprzęt sieci FR powinien spełnić pewne wymagania jeszcze nowocześniejszej technologii, jaką jest ATM. Chodzi o to, by sprzęt zastosowany w sieci FR umożliwiał segmentację ramek w krótkie komórki w celu ich transportowania w sieci, tak jak zakłada to technologia ATM.

Standard ATM jest pierwszym jednolitym systemem przesyłania informacji zarówno typowo telekomunikacyjnych, jak i informatycznych. Powoduje to uproszczenie pracy sieciowej dużych komputerów typu **mainframe**, komputerów osobistych i stacji roboczych, umożliwiając jednoczesną transmisję tekstów, danych, mowy i obrazów.

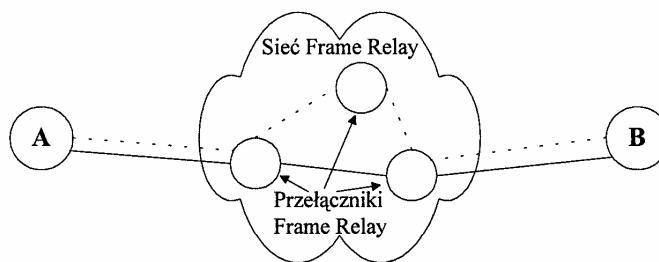
Potencjalne możliwości techniki ATM spowodowały gwałtowny wzrost zainteresowania działalnością międzynarodowej organizacji ATM Forum, która powstała w 1991 roku w USA. Obecnie organizacja ta skupia ponad 400 członków: producentów, operatorów sieci, instytuty naukowe, potencjalnych użytkowników wywodzących się z przemysłu i urzędów publicznych.

Celem działań organizacji ATM Forum jest wprowadzenie jednolitej światowej techniki i usług w sieci ATM oraz wspomaganie badania zapotrzebowania rynku przez szybkie wprowadzenie i prezentację nowych możliwości ATM.

Technika ATM jest często wprowadzana do istniejących sieci, których infrastruktury są oparte na wykorzystaniu bardzo różnych technologii. Zdolność komunikowania się (sprzęgania) nowej techniki z elementami "starej" ma bardzo istotne znaczenie z powodów ekonomicznych oraz ze względu na potrzebę psychologicznej akceptacji nowych rozwiązań.

Technika ATM jest wbudowana w świat publicznych sieci telefonicznych, sieci ISDN, sieci pakietowych (X.25 lub Frame Relay) oraz różnego typu sieci LAN i WAN. W związku z wprowadzaniem techniki ATM w infrastrukturę istniejących sieci należy wspomnieć, że istnieje ścisła współpraca pomiędzy grupami ATM Forum i Frame Relay Forum.

### 6.2.6 Struktura połączeń w sieci Frame Relay



Rys. 6.12. Nadmiarowa architektura Frame Relay

Sieć FR składa się z wielu fizycznych i logicznych dróg połączeniowych oraz przełączników FR - programów obsługi ramkowej, uaktywniających poszczególne kierunki i połączenia logiczne między węzłami. Połączenie między przełącznikami staje się aktywne dopiero po przydzieleniu mu identyfikatora połączenia danych DLCI (ang. *Data Link Connection Identifier*), co umożliwia realizację sieci wirtualnej o podwyższonej niezawodności, niekoniecznie związanej z konkretnym, fizycznym kanałem transmisyjnym pomiędzy dwoma użytkownikami. W celu uzyskania komunikacji pomiędzy dwoma abonentami (np. A i B na rys. 6.12) należy zestawić między nimi połączenie logiczne złożone z aktywnych kanałów logicznych między parami przełączników (np. połączenie na rys. 6.12, zaznaczone linią ciągłą). FR realizuje bowiem usługi typu połączeniowego. Wzrost niezawodności uzyskuje się przez możliwość automatycznego tworzenia alternatywnych ścieżek wirtualnych, łączących wybrane węzły lub punkty docelowe w sieci. Połączenia zaznaczone, na rys. 6.12, liniami ciągłą i przerywaną zapewniają opcjonalną komunikację między stacjami A i B. Należy podkreślić, że w tym samym czasie aktywne może być tylko jedno z połączeń opcjonalnych. Gdy kanał logiczny przestaje być potrzebny, następuje jego "likwidacja"; oznacza to, że identyfikatory DLCI, używane dotychczas przez ten kanał, stają się dostępne dla innych połączeń.

W sieci FR mogą występować trzy typy połączeń wirtualnych:

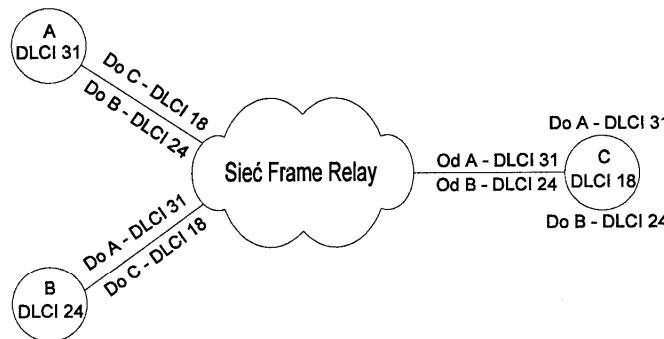
- Stałe połączenia wirtualne PVC (ang. *Permanent Virtual Circuit*) przydzielane w trakcie subskrypcji przed komunikacją, a następnie dostępne przez dłuższy czas (mesiące, lata). Z punktu widzenia użytkownika takie połączenie spełnia funkcję prywatnej linii dzierżawionej o stałym opóźnieniu transmisji. W razie awarii tworzona jest droga zastępcza, omijająca uszkodzony fragment sieci;
- Przełączane połączenia wirtualne SVC (ang. *Switched Virtual Circuit*) zestawiane i komutowane na żądanie abonenta; Jest to połączenie, typu "punkt-punkt", stanowiące analogię do komutowanych połączeń telefonicznych;
- Grupowe połączenia wirtualne (ang. *Multicast*) zestawiane również na dłuższy okres, zezwalające dodatkowo na równoczesny dostęp wielu użytkowników sieci FR do tych samych zasobów sieci. Ten typ połączeń umożliwia dostarczanie kopii wszystkich ramek wybranej grupie abonentów, zwykle w zastosowaniach rozsiewczych.

### 6.2.7 Adresowanie w sieci Frame Relay

Pierwotny tryb adresowania w technologii FR opierał się na założeniu, że wszystkie adresy DLCI mają znaczenie wyłącznie lokalne. Każde urządzenie użytkownika mogło wysyłać dane do odbiorcy, znając tylko lokalny numer kanału. Oznaczało to, iż odbiorca mógł być widziany przez dwóch nadawców pod zupełnie innymi adresami DLCI. Ten tryb został zatem nazwany adresowaniem lokalnym. Jednak jego implementacja w praktyce okazała się bardzo trudna. Z tego względu Frame Relay Forum, jako jedno z pierwszych zaleceń, wprowadziło alternatywny tryb adresowania, oparty na globalnym znaczeniu adresów DLCI.

Podstawą tego adresowania stanowi fakt, iż każdy adres DLCI jest unikatowy w skali całej sieci i może pojawić się tylko raz jako adres urządzenia. Takie podejście znakomicie uprościło strukturę sieci i tworzenie połączeń.

Każda rama wchodząca do sieci FR posiada zarówno identyfikator DLCI jak i adres odbiorcy i wraz z nimi jest przesyłana poprzez węzły sieci. W punkcie wyjścia, czyli na styku z odbiorcą, adres DLCI jest zamieniany na adres nadawcy. W ten sposób odbiorca dowiaduje się, od kogo otrzymał ramek. Każde urządzenie użytkownika ma przypisany adres DLCI. Wszyscy, którzy chcą przesłać informację do wybranego odbiorcy, używają jednego i tego samego adresu. Opisany sposób adresacji przedstawia rysunek 6.13. W przypadku ramek adresowanych do urządzenia C zarówno A, jak i B używają adresu 18. Na rysunku 6.13 pokazano dodatkowo mechanizm zamiany adresów ramek, które napływają do C. W punkcie wyjścia z sieci FR rama z A otrzymuje adres 31 (stacji nadawczej), a rama z B, odpowiednio, adres 24. Przedstawiony tryb adresacji jest dużo prostszy w implementacji niż tryb adresacji lokalnej. W obecnej chwili wszyscy producenci sprzętu oferują urządzenia wyłącznie z globalnym trybem adresowania.



Rys. 6.13. Adresowanie globalne w sieci Frame Relay

### 6.2.8 Komutacja pakietów

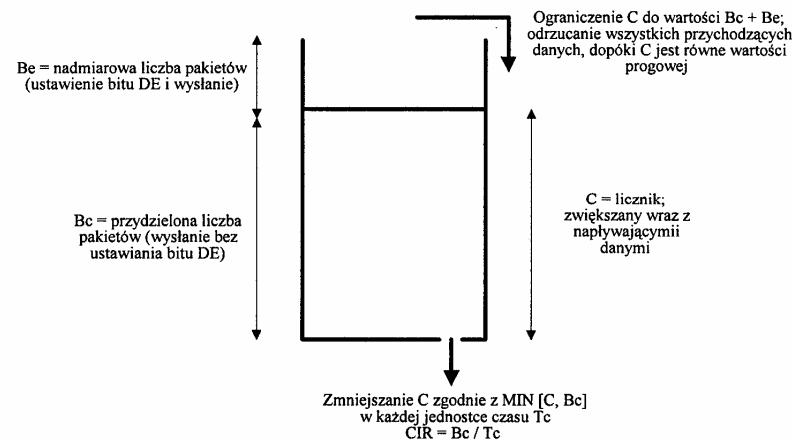
Najnowsze procedury komunikacyjne uwzględniają realizację połączeń przez światłowodowe media transmisyjne, z możliwością negocjowania wymaganej przepustowości informacyjnej CIR (ang. Committed Information Rate) - dla każdego połączenia wirtualnego. Dostawca usługi FR, organizujący połączenia typu PVC lub SVC wiążące dwa punkty w sieci, jest zobowiązany do utrzymania tego kanału oraz zapewnienia wynegocjowanych z usługobiorcą parametrów technicznych. Dzięki temu sieć z przełączaniem pakietów FR stała się w pełni siecią z szybką komutacją pakietów. Ramki użytkownika są przesyłane przez medium i urządzenia transmisyjne z maksymalną dostępną szybkością, natomiast w przerwach, wynikających z nieciągłości w transmisji, kanał i związane z nim urządzenia transmisyjne mogą być wykorzystywane do innych usług - o odpowiednio mniejszym wskaźniku CIR. Sumaryczna wartość wynegocjowanych wskaźników CIR dla różnych usług lub abonentów korzystających z tego samego kanału transmisyjnego nie może przekroczyć średniej dostępnej przepustowości informacyjnej oferowanej przez dane medium transmisyjne.

Wartość parametru CIR stanowi oszacowanie przez użytkownika wielkości jego ruchu w okresie zajętości. Ustalenie przez sieć wartości współczynnika CIR, który jest mniejszy lub równy od żądanego przez użytkownika, jest zobowiązaniem sieci do dostarczenia danych z tą szybkością bez wystąpienia błędów. Program obsługi ramkowej, do którego dołączona jest stacja użytkownika, spełnia funkcję „dozownika”. Jeśli użytkownik wysyła dane z szybkością mniejszą niż CIR, to wyjściowy program obsługi nie podejmuje żadnych działań, w szczególności nie dokonuje modyfikacji specjalnego bitu DE (ang. Discard Eligibility), sygnalizującego pojawienie się ramki „nadmiarowej”. Jako bit DE, informujący o możliwości odrzucenia ramki, wykorzystuje się przy tym jeden z bitów pola adresowego ramki. Sygnali-

### 6.2 Podstawy Standardu Frame Relay

zuje on pierwszeństwo w odrzuceniu ramki (w stosunku do ramek, w których bit ten nie jest ustawiony) w sytuacji, gdy konieczne staje się odrzucenie pewnych ramek. Jeśli szybkość transmisji przewyższa wartość CIR, to program obsługi ramkowej przesyła wszystkie nadmiarowe ramki z ustawionym bitem DE. Ramki te mogą przedostać się przez sieć lub mogą być odrzucone, jeśli natkną się na stan przeciążenia w sieci. Maksymalna szybkość transmisji w sieci FR jest określona tak, by wszystkie ramki powyżej pewnego progu były odrzucane na wejściu programu obsługi.

Procedura ta, w teorii, winna być realizowana w sposób ciągły. W praktyce możliwym przybliżeniem, dla programu obsługi ramkowej, jest pomiar ruchu każdego połączenia logicznego w przedziale czasu  $T_C$ . Stosownie do tego muszą być negocjowane dwa dodatkowe parametry. Pierwszym jest przydzielana połączeniu liczba paczek  $B_C$  (ang. committed burst size) określająca maksymalną ilość danych, które sieć zobowiązuje się dostarczyć połączeniem logicznym w czasie  $T_C$ . Drugi parametr stanowi nadmiarowa liczba paczek  $B_e$  (ang. excess burst size). Jest to maksymalna ilość danych, o której użytkownik może przekroczyć wartość  $B_C$ , w przedziale  $T_C$ ; dane te zostaną jednak dostarczone z prawdopodobieństwem mniejszym, niż dane w ramach  $B_C$ . Oznacza to, że sieć FR podejmie próbę przesłania tych danych, lecz bez gwarancji dostarczenia ich do adresata (zgodnie z zasadą „best effort”). Przykładowo, jeśli mamy połączenie fizyczne 2 Mb/s do przełącznika FR i opakowany kanał wirtualny o parametrach  $B_C = 64$  kb/s oraz  $B_e = 512$  kb/s, to sieć podejmie próbę przeniesienia chwilowego ruchu do wartości 576 kb/s.



Rys. 6.14. Algorytm przeciekającego wiadra

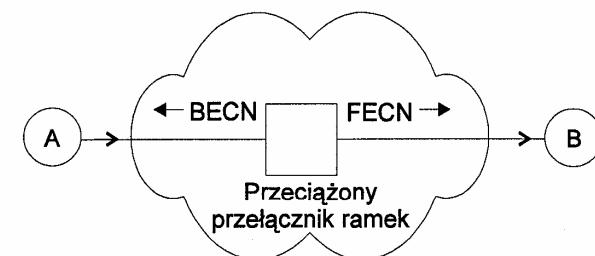
Specyfikacja ANSI zaleca użycie algorytmu przeciekającego wiadra (ang. *leaky-bucket algorithm*) w celu monitorowania przepływu danych (rysunek 6.14). Program obsługi ramkowej rejestruje, za pośrednictwem licznika  $C$ , liczbę danych wysyłanych przez każdego z użytkowników. Licznik ten jest zmniejszany o wielkość  $B_C$  w każdym przedziale czasu  $T_C$ . Oczywiście, wartość licznika nie może być ujemna, tak więc prawdziwe jest  $C \leftarrow \text{MIN}[C, B_C]$ . Ilekroć wartość licznika przewyższy  $B_C$ , ale jest mniejsza niż  $B_C + B_e$ , to napływanące ramki przekraczające przydzieloną liczbę pakietów, są wysyłane z ustawionym bitem DE. Jeśli licznik osiągnie wartość  $B_C + B_e$ , wówczas wszystkie następujące napływanące ramki są odrzucane, dopóki wartość licznika nie zostanie zmniejszona do pożądanego poziomu. Pomimo rygorystycznego kontrolowania przez przełączniki FR zasady przydzielania i egzekwowania wskaźników CIR, dla poszczególnych usług mogą w praktyce zaistnieć przeciążenia w pracy przełącznika. Są to następujące sytuacje:

- Przekraczanie przez użytkowników uzgodnionych i przydzielonych im wskaźników przepustowości informacyjnej CIR;
- Użytkownicy, nie przekraczając przepustowości przyznanej im przez wskaźniki CIR, transmitują okresowo (ale równocześnie) z pełną szybkością swoich portów nadawczych;
- W razie awarii części sieci mogą zaistnieć zmiany dróg przesyłania, powodujące z kolei przeciążenie innych, sąsiadujących przełączników FR znajdujących się na trasie alternatywnej.

### 6.2.9 Mechanizm informowania o przeciążeniu

*W przypadku przeciążenia przełącznika, pośredniczącego w przekazie ramek, inicjuje on realizację specjalnej procedury ochronnej*, informując o tym stanie nadawcę za pośrednictwem bitu BECN (ang. *Backward Explicit Congestion Notification*) oraz odbiorcę ramek, bitem FECN (ang. *Forward ECN*). Otrzymując ramkę z informacją FECN, użytkownik-odbiorca dowiaduje się, że kierunek, z którego ona właśnie przybyła, jest przeciążony. Powinien on w tym momencie podjąć kroki, które uwzględniają zwiększone opóźnienia lub zagubienie ramek. Nieuwzględnie ostrzeżenia o przeciążeniu spowoduje wysłanie - po upływie normalnego czasu oczekiwania - żądania retransmisji ramek (w przypadku braku odbioru ramek). Węzeł nadający zacznie więc generować dodatkowy ruch, blokując tym samym całkowicie strefę przeciążoną. Prawidłowa akcja, pozwalająca rozwiązać chwilowe problemy, powinna polegać na wydłużeniu czasów potwierdzeń i opóźnieniu generacji żądań retransmisji. W przypadku otrzymania ramki z bitem BECN, akcja podejmowana przez urządzenie nadające jest oczywista. Powinno ono zaprzestać lub radykalnie obniżyć intensywność wysyłania ramek w kierunku strefy przeciążenia. Na rysunku 6.15 pokazano sytuację przeciążenia przełącznika FR, przy czym przeciążenie to występuje na kierunku od A do B. W tym przypadku ramki docierające do węzła A mają ustawiony bit BECN. Z kolei ramki docierające

„zgodnie” z kierunkiem przeciążenia do węzła B ostrzegają użytkownika adresata za pomocą bitu FECN.



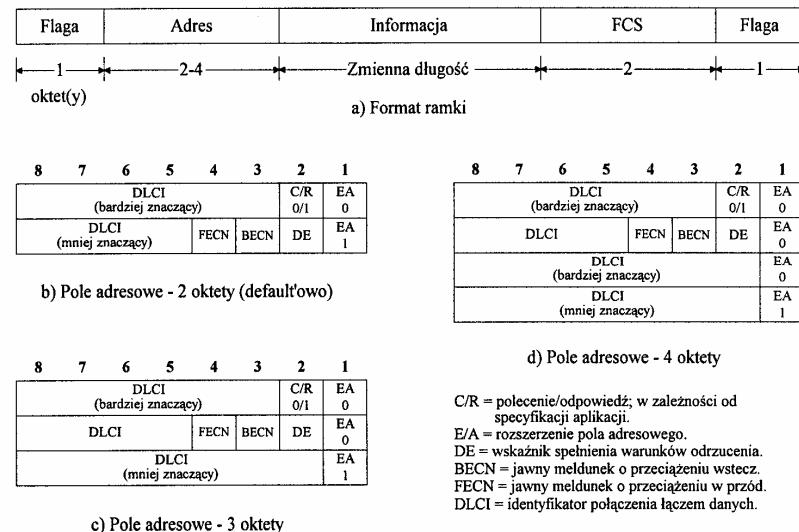
Rys. 6.15. Przeciążenie przełącznika Frame Relay

Stosowanie w sieci FR znacznie lepszych jakościowo linii transmisyjnych (światłowody) redukuje konieczność kontroli i retransmisji uszkodzonych ramek w każdym z kolejnych węzłów sieci, skracając czas ich komutacji w węzłach nawet poniżej 2 ms. Pomimo, że przełączniki FR mają mechanizmy kontrolne (zapewniające detekcję poprawności transmitowanych ramek), za korektę i retransmisję brakujących lub uszkodzonych ramek odpowiadają wyłącznie przełączniki końcowe lub bezpośrednio sprzęt użytkownika, przyłączany do węzła w sieci.

Mechanizm współpracy stacji końcowej z siecią FR polega na zamianie pakietu informacyjnego w stacji nadawczej na ramek, które po uzupełnieniu o identyfikatory połączeń DLCI (adresujące odpowiednie ścieżki wirtualne), po obliczeniu sekwencji kontrolnej oraz uzupełnieniu o flagi są przesyłane przez sieć FR. Węzeł lub stacja docelowa realizują proces odwrotny: potwierdzają zgodność sekwencji ramek, usuwają nagłówek i przesyłają informację właściwą do użytkownika lub inicują proces retransmisji, w przypadku błędu.

### 6.2.10 Struktura ramki FR

Informacje są przesyłane w sieci FR w postaci ramek (rysunek 6.16) o zmiennej długości części informacyjnej, zgodnie z zaleceniem Q.921. Każda rama jest ograniczona dwiema flagami (ang. *flags*): otwierającą i zamykającą, pomiędzy którymi są umieszczone nagłówki (ang. *header*), właściwa informacja i pole kontrolne FCS (ang. *Frame Check-Sequence*). Rozmiar ramki, z uwzględnieniem pola informacyjnego ramki, jest definiowany w fazie ustalania połączenia i zależy od rodzaju usługi przekazywanej przez sieć. Stosowane są nagłówki o różnej długości: 2-, 3- i 4-bajtowe, mające swoje odwzorowanie w protokołach LAP F warstwy łączna danych modelu odniesienia ISO-OSI dla protokołów FR. W celu efektywnej realizacji procedur kontrolnych wskazane jest używanie ramek o stałej liczbie oktetów.



Rys. 6.16. Formaty ramek Frame Relay

### 6.2.11 Organizacja usług FR

Zbliżone funkcje sieci pakietowych X.25 oraz FR umożliwiają wzajemne funkcjonowanie obydwu typów usług w tym samym medium transmisyjnym, przybierając różne formy współpracy:

- Wykorzystanie tych samych zasobów komutacyjnych o różnym oprogramowaniu i tej samej architekturze zarządzania;
- Zastosowanie wspólnej infrastruktury transmisji, lecz z rozdziałem kanałów; organizowanej z wykorzystaniem infrastruktury 2 Mb/s, z wprowadzeniem multiplekserów statystycznych w sieci rdzeniowej (szkieletowej);
- Dzielenie w sposób dynamiczny wspólnej infrastruktury transmisyjnej między obie usługi: X.25 i FR, w zależności od potrzeb użytkowników.

Wdrożenie usług FR w sieciach PSPDN daje wiele korzyści, niedostępnych w sieciach z protokołem X.25. Najważniejsze z nich to:

- Realizacja usług FR przez styki transmisyjne o różnej przepływności wymagane przez użytkowników stosujących wielorakie protokoły: 144 kb/s dla V.35, do 1920 kb/s na styku V.24 - V.11 i X.24 oraz 2048 kb/s na styku G.703. Dotyczy to również protokołów X.25, X.28 oraz SNA/SDLC;
- Znacznie uproszczona komutacja ramek, zapewniająca ograniczenie czasów opóźnień. Przy dobrej jakości łącz cyfrowych w węzłach pośredniczących analizowane są tylko pola adresowe, co znacznie skraca czas obsługi ramek w węzłach. Technika FR jest więc szczególnie efektywna przy

przesyłaniu długich pakietów (około 4096 oktetów) łączami transmisyjnymi o dobrej jakości;

- Tworzenie szybkich wirtualnych sieci prywatnych w celu łączenia różnych fragmentów sieci LAN, udostępnianych dynamicznie wybranym użytkownikom;
- Spełnienie podstawowych wymagań odnośnie współpracy z najnowszą technologią ATM przez segmentację ramek, aż do wielkości pojedynczej komórki, będącej podstawą transportu w asynchronicznych sieciach ATM, zarówno w nakładkowym trybie pracy na innych systemach komunikacyjnych, jak i w jednolitej docelowej postaci ATM.

Frame Relay zostało stworzone jako alternatywa dla X.25 i stanowi dobrze zdefiniowany protokół komutacji pakietów. Rezygnując z potwierdzeń na każdym etapie transmisji (obecnych w X.25) zapewniono środki do realizacji szybkiej transmisji danych, dostępnej we współczesnych sieciach. Protokół FR zakłada zmienną długość ramek oraz tworzenie połączeń logicznych, czyli tzw. kanałów wirtualnych i podobnie jak X.25 definiuje styl między użytkownikiem, a siecią na zasadach DTE/DCE.

Zgodnie z założeniami protokołu FR, nie znalazły się w nim procedury kontroli przepływu danych, kolejności ramek, i ich odtwarzania. Problemy te zostały przeniesione na poziom wyższych warstw, upraszczając i przyspieszając sam proces przekazywania ramek. Jedyną „akcją” spowodowaną wykryciem błędного bitu jest odrzucenie całej ramki. Decyzja o retransmisji należy do urządzeń końcowych. Sieć FR w porównaniu z wcześniejszymi rozwiązaniami sieci pakietowych “traci” swoją inteligencję na rzecz urządzeń końcowych użytkownika. Ta “pozorna” strata procentuje w postaci minimalnych opóźnień przełączania.

Adresowanie systemu końcowego i multipleksowanie połączeń odbywają się w FR w warstwie 2-giej, eliminując w ten sposób jedną warstwę w procesie przetwarzania. Prostota protokołu Frame Relay wynika z braku mechanizmów tradycyjnej kontroli błędów i sterowania przepływem danych. Brak tych mechanizmów sprawia jednakże, iż sieć FR jest podatna na przeciążenia. Jest to częściowo kompensowanie przez zastosowanie prostego mechanizmu unikania przeciążenia i mechanizmu wychodzenia ze stanu przeciążenia, które te mechanizmy są wbudowane w ten protokół.

Reasumując: FR jest technologią „środka” ulokowaną pomiędzy wolną techniką komutacyjną X.25, a nową wizją sieci, kierowaną przez technologię ATM. FR zapewnia zadawalające rozwiązania na dziś i łatwą migrację do przyszłych technologii.

## 7 Asynchroniczny przekaz danych - ATM

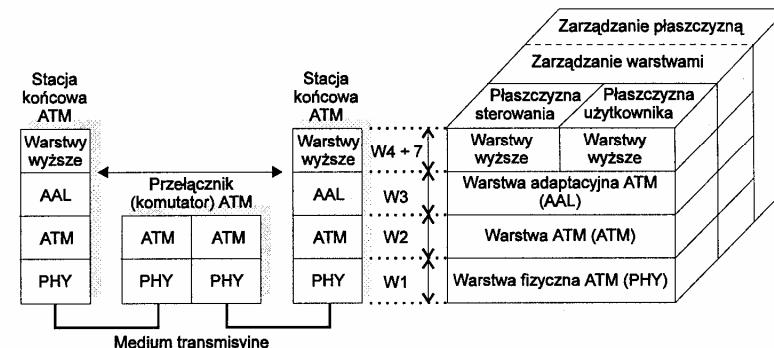
*Technika asynchronicznego przekazu danych ATM* (ang. *Asynchronous Transfer Mode*) została zaakceptowana w 1988 roku przez ITU-T (ang. *International Telecommunications Union - Telecommunications Sector*) jako docelowa i standardowa technika komutacyjna dla sieci szerokopasmowej B-ISDN (ang. *Broadband-Integrated Services Digital Network*). Prace nad standardem B-ISDN ATM, zainicjowane przez CCITT (obecnie ITU-T), doprowadziły do opracowania niekonwencjonalnej metody zestawiania połączeń, sterowania dostępem do sieci i zarządzania jej zasobami. ATM nie definiuje przy tym konkretnego medium transmisyjnego wykorzystywanego do realizacji połączeń, dopuszczając użycie światłowodów, skrętek przewodowych UTP i STP, kabli koncentrycznych, a także kanałów bezprzewodowych (bezprzewodowe sieci ATM). W celu przyspieszenia prac standaryzacyjnych oraz szerszej promocji techniki ATM, grupa producentów sprzętu i firm świadczących usługi telekomunikacyjne stworzyła w 1991 roku organizację znawaną pod nazwą ATM Forum. Organizacja ta opracowuje dokumenty, mające znamiona standardów, będąc też wpływową grupą „nacisku”, silnie oddziaływaną na strategię rozwoju ATM. Prace ATM Forum obejmują opracowywanie zunifikowanych układów interfejsów sieciowych, definiowanie zasad zarządzania i sterowania ruchem, a także badanie przydatności różnych mediów transmisyjnych i metod testowania sprzętu ATM.

### 7.1 Architektura B-ISDN ATM

Dla sieci B-ISDN ATM opracowano technikę komutacji komórek, będącą szybką komutacją pakietów, realizowaną w trybie połączniowym, z wykorzystaniem połączeń wirtualnych zestawianych w fazie nawiązywania połączenia. *Cechą charakterystyczną ATM jest ujednolicenie postaci komutowanych jednostek danych dla wszystkich realizowanych w sieci usług.* W metodzie ATM przesyłane strumienie informacji dzielone są więc na jednakowe, znormalizowane bloki, nazywane komórkami. Komórka składa się przy tym z 53 bajtów.

Przekaz danych realizowany jest w postaci strumienia komórek, przy czym do realizacji usług wymagających małej przepływności wykorzystywana jest niewielka liczba komórek przesyłanych w jednostce czasu. Z kolei do realizacji usług wymagających dużej przepływności bitowej angażowana jest odpowiednio większa liczba komórek poddanych multipleksacji w szerokopasmowym kanale wyjściowym. Technika ta pozwala więc na osiągnięcie efektu skalowalności przepustowości, obserwowanego też np. w X.25, udostępnianej poszczególnym użytkownikom sieci.

Podobnie jak i w innych typach sieci telekomunikacyjnych, również i w systemie B-ISDN ATM protokoły realizujące funkcje sterowania, zarządzania i obsługi procesów użytkowych mają strukturę warstwową.



Rys. 7.1. Architektura B-ISDN ATM

Koncepcję warstwowej architektury standardu ATM dla sieci szerokopasmowej B-ISDN prezentuje rysunek 7.1. Model ATM składa się przy tym z warstw i płaszczyzn. Wyróżnia się trzy podstawowe warstwy. Są to:

- warstwa fizyczna (ang. *Physical Layer*) - definiująca funkcje związane z dostępem do medium transmisyjnego;
- warstwa ATM (ang. *ATM Layer*) - obejmująca funkcje zapewniające niezawodny przekaz komórek, bez względu na typ usługi;
- warstwa adaptacyjna bądź adaptacji ATM (ang. *ATM Adaptation Layer*) - realizująca typowe funkcje związane z segmentacją i składaniem jednostek danych wymienianych między wyższymi warstwami, a warstwą ATM, jak również wykrywanie błędów i podejmowanie stosownych reakcji na błędy w transmisji, rozpoznawanie brakujących lub niesekwencyjnych komórek, a także obsługę różnych klas ruchu.

Funkcje poszczególnych warstw modelu ATM przytoczone są w tabeli 7.1. W modelu definiowane są też „płaszczyzny” o budowie warstwowej, wśród nich wyróżnia się:

- płaszczyznę użytkownika (ang. *User Plane*) - odpowiedzialną za przekaz informacji użytkownika poprzez sieć ATM i sterowanie przepływem strumieni informacji;
- płaszczyznę sterowania (ang. *Control Plane*) - odpowiedzialną za realizację wywołań oraz nadzór nad jakością połączeń; w płaszczyźnie tej zawarte są funkcje sygnalizacyjne związane z zestawianiem, nadzorem oraz rozłączaniem połączeń;

- płaszczyznę zarządzania (ang. *Management Plane*) - odpowiedzialną za realizację funkcji nadzoru nad siecią ATM; w płaszczyźnie tej definiowane są funkcje zarządzania warstwami (ang. *Layer Management*) oraz funkcje zarządzania płaszczyzną (ang. *Plane Management*).

Tabela 7.1. Funkcje warstw B-ISDN

	Funkcje wyższych warstw	Wyższe warstwy	
zarządzanie	Tworzenie bloków danych o właściwej długości poprzez: <ul style="list-style-type: none"> <li>grupowanie bitów lub bajtów ewentualnie wydłużanie pakietów,</li> <li>tworzenie nagłówków i/lub zakończeń bloków,</li> <li>generowanie ewentualnych zabezpieczeń CRC</li> </ul>	CS	warstwa adaptacyjna AAL <i>(ATM Adaptation Layer)</i>
	Podział bloków na segmenty; Tworzenie nagłówków i/lub zakończeń segmentów; Generowanie zabezpieczeń CRC; Ewentualne multipleksowanie połączeń.	SAR	
Tworzenie komórek; Generowanie i wydzielanie nagłówków; Nawiązywanie i kasowanie połączeń; Translacja pól VPI/VCI (identyfikatora ścieżki logicznej/identyfikatora kanału logicznego); Multipleksowanie i demultipleksowanie komórek; Sterowanie ruchem - kontrola przepływu komórek (GFC); Obsługa wielu klas QoS.		warstwa ATM <i>(ATM Layer)</i>	
warstwami	Dopasowywanie szybkości transmisji komórek; Weryfikacja nagłówków w komórkach; Wydzielanie komórek ze strumienia bitów; Adaptacja strumienia komórek do struktury ramki transmisyjnej; Gencrowanie i odtwarzanie ramek systemu transmisyjnego.	TC	warstwa fizyczna <i>(Physical Layer)</i>
	Odtwarzanie podstawy czasu; Transmisja bitów; Fizyczny dostęp do medium.	PM	

Objaśnienie skrótów zawartych w tabeli:

warstwa adaptacyjna AAL ATM - *ATM adaptation layer*  
podwarstwa zbieżności CS - *Convergence Sublayer*

podwarstwa medium fizycznego PM - *Physical-Medium sublayer*

podwarstwa segmentacji i składania SAR - *Segmentation-And-Reassembly sublayer*

podwarstwa zbieżności transmisji TC - *Transmission-Convergence sublayer*

## 7.2 Warstwa fizyczna

Funkcje zarządzania warstwami realizują zarządzanie zasobami oraz parametrami obiektów specyfikowanych w protokołach, zapewniają one przepływ informacji typu „działanie i utrzymanie” (ang. *OAM - Operations, Administration and Maintenance*) w odniesieniu do konkretnej warstwy.

Z kolei funkcje zarządzania płaszczyzną koordynują pracę systemu jako całości, jak też zapewniają współpracę międzypłaszczyznową.

Opis modelu odniesienia protokołu B-ISDN ATM zawarty jest w zaleceniu CCITT I.121 z roku 1988.

## 7.2 Warstwa fizyczna

Podstawowe funkcje warstwy fizycznej zostały podane w tabeli 7.1. Należą do nich między innymi: wyodrębnianie nagłówków komórek, wydzielanie komórek ze strumienia bitów, adaptacja strumienia komórek do struktury ramki systemu transmisyjnego i odtwarzanie podstawy czasu. Funkcje te realizowane są przez jedną z dwóch podwarstw warstwy fizycznej:

- podwarstwę medium fizycznego - PM,
- podwarstwę zbieżności transmisji - TC.

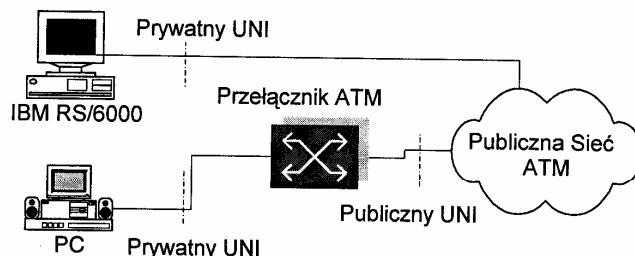
Podwarstwa medium fizycznego jest przy tym odpowiedzialna za poprawną transmisję i odbiór bitów. Zapewnia ona fizyczny dostęp do medium transmisyjnego, określa charakterystyki tego medium, parametry nadajnika i odbiornika, kod transmisyjny, strukturę ramkowania, itp. Drugą podwarstwą w warstwie fizycznej jest podwarstwa zbieżności transmisji odpowiedzialna za dopasowanie napływających danych do struktury ATM. Podwarstwa ta otrzymuje komórki z warstwy ATM i przekształca je do postaci odpowiedniej do transmisji przez podwarstwę medium fizycznego. Po stronie odbiorczej podwarstwa zbieżności dokonuje wydzielenia komórek ze strumienia bitów lub bajtów, otrzymanego z podwarstwy medium fizycznego, weryfikuje ich nagłówki, sprawdza poprawność transmisji komórek i dostarcza poprawne komórki do warstwy ATM. Okresy czasu, w których nie są przesyłane komórki z danymi podwarstwa PM wykorzystuje do przesyłania komórek zarządzających (ang. *Management Cells*). Komórki takie nie są przepuszczane do warstwy ATM. Identyfikuje się je na podstawie postaci nagłówka, która nie jest dozwolona dla zwykłych komórek ATM.

Interesującą cechą warstwy fizycznej ATM jest to, iż nie definiuje ona żadnej konkretnej techniki transmisji, ani też typu medium transmisyjnego. ATM pozwala na stosowanie różnych mediów transmisyjnych w tym światłowodów, skrętek i kabli koncentrycznych. Z kolei jako technikę transmisji odpowiednią do zastosowań ATM eksperci wskazują systemy synchroniczne SDH (ang. *Synchronous Digital Hierarchy* - odpowiednik w USA - SONET - *Synchronous Optical Network*).

### 7.2.1 Rodzaje interfejsów fizycznych

W wyniku prac standaryzacyjnych prowadzonych przez ITU-T oraz działań podejmowanych przez ATM Forum zdefiniowano szereg układów stykowych. Dwa podstawowe rodzaje styków (interfejsów) fizycznych to:

1. styk użytkownik-sieć UNI (ang. *User-Network Interface*) określający zasady połączenia stacji komputerowej użytkownika z siecią ATM. Istnieją przy tym dwa rodzaje interfejsów UNI: prywatny UNI i publiczny UNI (patrz rysunek 7.2). Pierwszy z nich odnosi się do styku pomiędzy użytkownikiem, a systemem komutacyjnym - komutatorem ATM, należącym do tej samej korporacji (sieci) co użytkownik. Drugi interfejs, nazywany publicznym UNI, wykorzystywany jest, gdy użytkownik łączy się z publiczną siecią ATM. Z interfejsem tym związany jest protokół ILMI (ang. *Interim Local Management Interface*). Standardy UNI do zastosowań w sieciach publicznych obejmują:



Rys. 7.2. Prywatne i publiczne interfejsy UNI

- styk UNI formatu DS1 (T1) o przepływności 1.544 Mb/s dla kabla koncentrycznego,
- styk UNI formatu J-2 o przepływności 6.312 Mb/s dla kabla koncentrycznego,
- styk UNI formatu DS3 o przepustowości 44.736 Mb/s dla kabla koncentrycznego,
- styki UNI formatów STS-1, STS-3c i STS-12 o przepływnościach 51.840 Mb/s, 155.520 Mb/s oraz 622.080 Mb/s dla światłowodów jednomodowych.

Z kolei standardy prywatnych styków UNI obejmują styki:

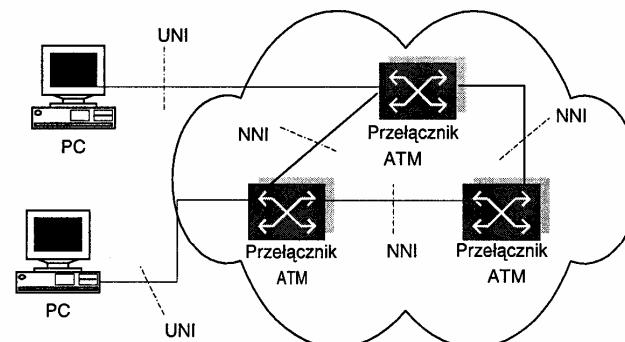
- CellStream o przepływności 25.6 MBodów dla skrętki UTP 3 kategorii,
- STS-1 o przepływności 51.84 Mb/s dla skrętki UTP 3 kategorii, światłowodu bądź koncentryka,
- FDDI (TAXI) o przepływności 100 Mb/s dla światłowodu wielomodowego,

- STS-3c o przepływności 155.520 Mb/s dla skrętki UTP-5, światłowodu bądź koncentryka,
- CellStream o przepływności 155.520 Mb/s (194.4 MBodów) dla światłowodów wielomodowych lub kabli koncentrycznych.

ATM Forum zapowiada kontynuowanie prac w zakresie styków UNI w warstwie fizycznej. Mają one doprowadzić do opracowania wersji styku UNI kompatybilnej z europejskimi traktami cyfrowymi 139.264 Mb/s i 34.368 Mb/s. Wykaz mediów i systemów transmisyjnych wraz z realizowanymi w nich szybkościami transmisji zestawiono w tabeli 7.2.

Tabela 7.2. Media fizyczne i szybkości transmisji

Typ ramki transmisyjnej	Szybkość transmisji [Mb/s]	Medium transmisyjne				
		światłowód wielomodowy	światłowód jednomodowy	kabel koncentryczny	skrętka UTP 5	skrętka UTP 3
DS1	1.544			•		
E1	2.048			•		
DS3	45			•		
E3	34			•		
Desktop ATM25	25.6					•
STS1	51					•
STS3c/STM1	155	•	•	•	•	•
STS12c/STM4	622	•	•			
4B/5B (TAXI)	100	•				
8B/10B (światłowód)	155	•				•



Rys. 7.3. Interfejsy NNI i UNI w sieci ATM

2. styk sieć-sieć NNI (ang. *Network-Node Interface*) opisujący zasady łączenia komutatorów ATM i odpowiadający głównie za zarządzanie ich współpracą. W przypadku NNI możemy także wyróżnić dwa rodzaje styków: NNI prywatny - dotyczący komutatorów w prywatnych sieciach oraz NNI publiczny.

ny, stosowany w sieciach publicznych. Z interfejsami typu NNI, zilustrowanymi na rysunku 7.3, związany jest protokół P-NNI.

Wspomniany powyżej protokół ILMI odpowiedzialny jest za autokonfigurację wielu parametrów protokołu ATM, np. wyznaczanie adresów serwerów inicjujących różne protokoły sieciowe ATM, czy też określanie adresów ATM stacji końcowych. Mechanizm rejestracji adresów ATM w standardzie ILMI pozwala systemom komutacyjnym (komutatorom) ATM rezerwować początkową część adresu stacji końcowych, podczas gdy pozostała część stanowi unikatowy 48 bajtowy adres MAC stacji. Protokół ten umożliwia administratorowi sieci kontrolę zarezerwowanych adresów.

Protokół P-NNI definiuje zbiór reguł routingu oraz sterowania obejmujących zasady ustalania połączenia z gwarancją jakości usług QoS (ang. *Quality of Service*), z uwzględnieniem: dostępnej w danej chwili przepustowości, obciążenia sieci i średniego opóźnienia transmisji. Jednocześnie protokół P-NNI umożliwia komutatorom ATM wymianę informacji o dostępnych adresach w sąsiednich przełącznikach oraz metryk QoS. Wymiana informacji pomiędzy przełącznikami ATM, z wykorzystaniem protokołu P-NNI, umożliwia zestawienie połączenia tak, by został osiągnięty pożądany poziom QoS oraz by uniknąć przeciążeń w sieci.

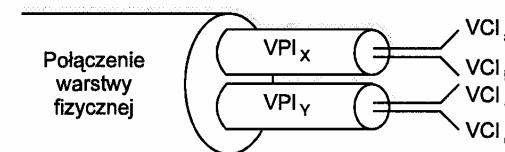
Protokół P-NNI jest stosowany zarówno w małych, lokalnych sieciach ATM, jak i w sieciach o zasięgu globalnym. Jest to możliwe dzięki hierarchicznemu podziałowi urządzeń w sieci na poziomy i grupy. W jednej grupie znajduje się przy tym liczba przełączników dobrana tak by zapewnić zarówno wysokie wykorzystanie przepustowości łącz jak i właściwe metryki QoS połączeń.

### 7.3 Warstwa ATM

Podstawowymi funkcjami warstwy ATM (patrz tabela 7.1) są: multipleksowanie i demultipleksowanie komórek, translacja pól VPI/VCI oraz sterowanie ruchem. W dalszej części przedstawimy strukturę komórki ATM, zasady realizacji połączeń typu VP i VC, a także typy i klasy usług warstwy ATM.

#### 7.3.1 Połączenia typu kanału logicznego i ścieżki logicznej

Podstawową jednostką danych przesyłaną w systemie B-ISDN ATM jest 53 bajtowa komórka. Komórki przesyłane są przez uprzednio zestawione połączenia logiczne. Definiuje się przy tym połączenia typu kanał wirtualny VCC (ang. *Virtual Channel Connection*) i ścieżka wirtualna VPC (ang. *Virtual Path Connection*). Połączenia typu VCC i VPC są jednokierunkowe i są zestawiane pomiędzy dwoma użytkownikami końcowymi (VCC) lub komutatorami ATM (VPC). Połączenie typu VPC definiuje się jako grupę kanałów VCC łączących te same węzły końcowe. Ścieżki i kanały są rozróżniane za pomocą identyfikatorów: ścieżki wirtualnej VPI (ang. *Virtual Path Identifier*) i kanału wirtualnego VCI (ang. *Virtual Channel Identifier*) umieszczonego w nagłówku komórki.

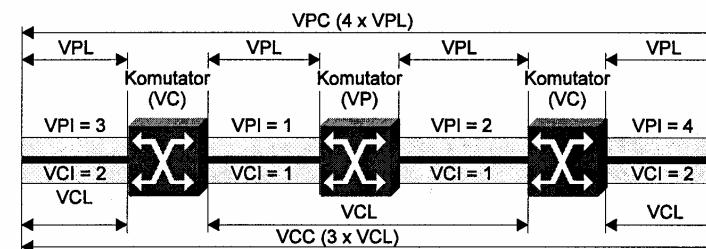


Rys. 7.4. Kanały i ścieżki wirtualne

Zaznaczone na rysunku 7.4 kanały wirtualne, opisane identyfikatorami VCI<sub>a</sub>, VCI<sub>b</sub>, VCI<sub>c</sub> oraz VCI<sub>d</sub> stanowią grupę kanałów VCC wchodzących w skład dwóch ścieżek wirtualnych. Identyfikatory VCI<sub>a</sub> i VCI<sub>b</sub> reprezentują przy tym dwie możliwe wartości identyfikatorów VCI wewnętrznej ścieżki VP o wartości VPI<sub>x</sub>. Identyfikatory VPI<sub>x</sub> i VPI<sub>y</sub> odpowiadają dwóm możliwym wartościami identyfikatorów VPI wewnętrznej połączenia warstwy fizycznej. Wartości identyfikatorów VCI są unikatowe jedynie w obrębie ścieżki wirtualnej.

Konkretnie połączenie logiczne jest zatem identyfikowane przez parę numerów: VPI i VCI. Tym samym otrzymuje się dwupoziomową hierarchię połączeń, obejmującą połączenia typu kanału wirtualnego VCC i ścieżki wirtualnej VPC.

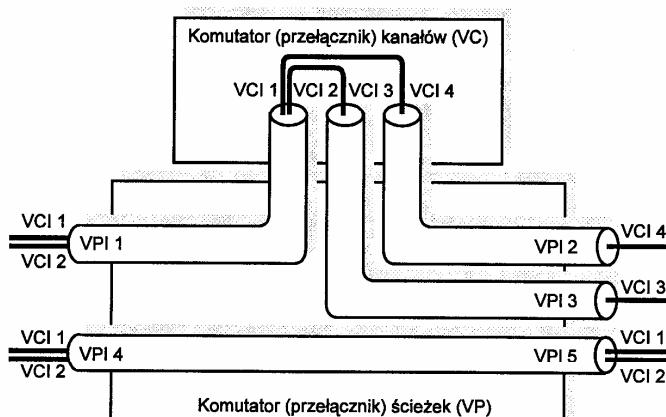
Na poziomie kanału wirtualnego (VC) połączenie logiczne VCC składa się z segmentów nazywanych łączami typu kanał wirtualny VCL (ang. *Virtual Channel Link*). Segmente te rozciągają się pomiędzy tymi węzłami (komutatorami) sieci, w których następuje zmiana wartości identyfikatora VCI. Z kolei na poziomie ścieżek wirtualnych, łączą typu VCL są realizowane poprzez połączenia typu VPC, które składają się z łącz typu ścieżka wirtualna VPL (ang. *Virtual Path Link*). Analogicznie do VCL, łączą te rozciągają się pomiędzy tymi węzłami sieci, w których następuje zmiana wartości pola VPI; ilustruje to rys. 7.5.



Rys. 7.5. Ilustracja połączeń VPC i VCC

Użycie ścieżek wirtualnych zwiększa efektywność i szybkość komutacji, redukując wielkość lokalnych tablic translacji komutatorów ATM poprzez grupowanie połączeń typu VCI. Brak konieczności zestawiania połączeń w węzłach pośrednich, przez które przebiega dana ścieżka, wpływa z kolei na przyspieszenie procedury ustanawiania nowego połączenia, wykorzystującego ścieżki wirtualne.

Transmisja danych odbywa się z udziałem systemów komutacyjnych (komutatorów) ATM. Rozróżniamy przy tym dwa podstawowe rodzaje komutatorów. Są to komutatory ścieżek VP i komutatory kanałów VC (por. rysunek 7.6). W komutatorze VP „znajdują się” zakończenia ścieżek wirtualnych. W związku z tym w urządzeniu takim dokonywana jest zamiana wartości VPI ścieżki wchodzącej na VPI ścieżki wychodzącej, według adresu docelowego danego połączenia. Z kolei w komutatorze kanałów, VC, translacji ulegają wartości zarówno wskaźników VCI jak i VPI.



Rys. 7.6. Komutatory ścieżek i kanałów

### 7.3.2 Komórka ATM

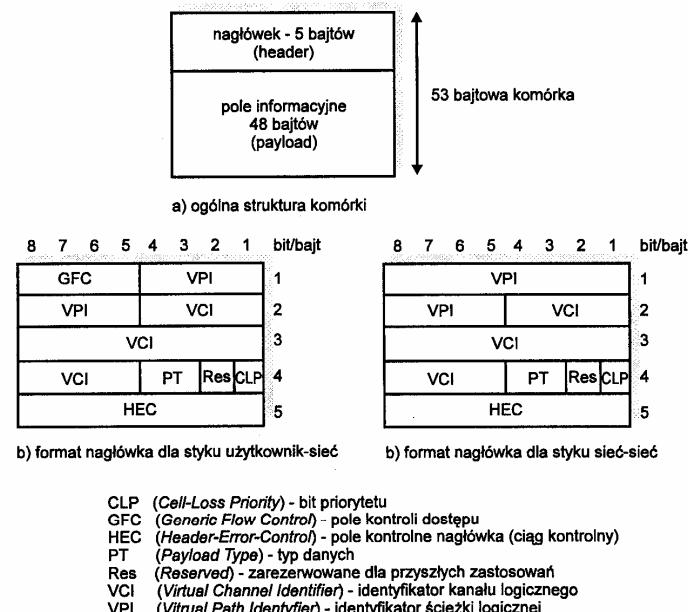
W systemach ATM stosuje się komórki o stałym rozmiarze. Komórka ma długość 53 bajtów, z czego 48 bajtów stanowi pole danych (zawartość informacyjna komórki, ang. *payload*), a 5 pozostałych tworzy nagłówek (patrz rysunek 7.7).

Stała długość komórki ATM ma szereg zalet, między innymi:

- opóźnienia wynikające z pracy sieci, w tym procesów przełączania w przełącznikach ATM, dają się lepiej przewidywać w przypadku komórek o stałej długości;
- przetwarzanie komórek o stałej długości jest łatwiejsze oraz bardziej niezawodne i efektywne niż przetwarzanie pakietów o zmiennej długości;
- stała długość komórek umożliwia przetwarzanie równolegle, co również zwiększa szybkość pracy węzłów sieci.

Definiowane są dwa typy komórek. Są to: pokazana na rys. 7.7b komórka wymieniana na styku użytkownik-siec, oraz prezentowana na rys. 7.7c komórka dla styku siec-siec (o nieco odmiennym formacie nagłówka). W tym drugim przypadku pole

kontroli dostępu nie jest zachowane. Natomiast pole przenoszące numer ścieżki logicznej (VPI) jest rozszerzone z 8 do 12 bitów.



Rys. 7.7. Struktura komórki ATM i formaty jej nagłówków

Poniżej prezentujemy krótką charakterystykę poszczególnych pól nagłówka.

**Pole kontroli dostępu GFC** (ang. *Generic Flow Control*) - występuje tylko dla interfejsu UNI. Umożliwia wielu przyłączonym abonenckim stacjom roboczym korzystanie z tego samego interfejsu UNI w obrębie sieci prywatnej. W innych przypadkach pole to służy do określania klasy usługi, ułatwiając sterowanie przepływem informacji przez sieć dla różnych poziomów QoS. Zawartość tego pola nie ma na razie żadnego wpływu na ruch kierowany od strony sieci ATM do terminali użytkownika.

**Identyfikator ścieżki logicznej VPI** - opisuje logiczną grupę kanałów wirtualnych. Dla styku UNI możliwe jest utworzenie do 256 ścieżek wirtualnych, natomiast dla styku NNI - 4096.

**Identyfikator kanału logicznego VCI** - opisuje logiczne połączenie między dwoma urządzeniami ATM. Możliwe jest utworzenie do 65536 kanałów wirtualnych w obrębie jednej ścieżki wirtualnej.

**Typ danych PT** (ang. *Payload Type*) - określa, czy przesyłane są dane użytkownika, czy też dane kontrolne ATM. Jeśli pierwszy bit jest zerem, to komórka

przenosi dane użytkownika, jeśli jedynką, są to dane administracyjne OAM. Jeżeli komórka przenosząca dane użytkownika stwierdza przeciążenie sieci, to w miejsce drugiego bitu PLT wstawia jedynkę.

**Res** - pełni funkcję sygnału sterującego (User Signal) i może być wykorzystany np. do poinformowania o zakończeniu transmisji serii komórek.

**Bit priorytetu CLP** (ang. *Cell Loss Priority*) - sieć ATM wstawia w to pole jedynkę, gdy wysłanie komórki powoduje przekroczenie parametrów kontraktu uzgodnionych przed rozpoczęciem transmisji. Dla przełącznika ATM jest to znak, że w razie przeciążenia sieci komórka taka ma być usuwana najpierw, czyli przed komórkami o CPL=0.

**Pole kontrolne HEC** (ang. *Header Error Control*) - suma kontrolna pierwszych czterech bajtów nagłówka komórki ATM. Do zabezpieczania wykorzystywany jest wielomian generujący o postaci:  $x^8 + x^2 + x + 1$ .

### 7.3.3 Sterowanie dostępem i zarządzanie zasobami sieci

#### B-ISDN ATM

*W celu zagwarantowania efektywnej obsługi wszystkich użytkowników sieci B-ISDN ATM, opracowano mechanizmy zarządzania zasobami sieci, zdefiniowane w zaleceniu ITU-T I.371.*

W sieci ATM, na poziomie kanałów wirtualnych, realizowana jest statystyczna multipleksacja komórek. Tym samym połączenia wirtualne, realizowane w obrębie ścieżki wirtualnej, oddziaływują wzajemnie na siebie, a strumienie komórek generowanych przez jednego użytkownika mogą wpływać na jakość QoS obsługiwanych połączeń.

Optymalne wykorzystanie zasobów sieci, w powiązaniu z jednoczesnym zapewnieniem pożąданej jakości poszczególnych połączeń, wymaga efektywnych metod sterowania ruchem w sieci. Należy przy tym pamiętać, że sieć ATM projektowana jest z myślą o integracji ruchu generowanego przez różnorodne aplikacje sieciowe, od asynchronicznego przekazu danych, w ramach usługi poczty elektronicznej czy też przesyłania zbiorów, po izochroniczny przekaz mowy bądź obrazów ruchomych we współczesnych aplikacjach multimedialnych.

Definiując mechanizmy sterowania ruchem w sieci ATM musimy więc uwzględnić szereg cech, wśród których najistotniejsze to:

- **duża szybkość transmisji** w sieci ATM, powodująca, że czasy propagacji w łączu stają się większe od czasów transmisji komórek;
- **duże różnice charakterystyk tzw. profili ruchu** generowanego przez różne aplikacje sieciowe, utrudniające optymalne wykorzystanie zasobów sieci;
- **różnicowanie wymagań jakościowych** związanych z realizacją różnych aplikacji;
- **odmiенноśc wewnętrznych własności źródeł**, w szczególności możliwość lub brak możliwości adaptowania charakterystyk ruchowych źródeł do zmian obciążenia w sieci ATM.

**Metody sterowania ruchem w sieci ATM klasyfikowane są jako prewencyjne bądź reakcyjne.**

**Sterowanie prewencyjne ma na celu zabezpieczenie sieci przed jej wejściem w stan przeciążenia, mogący doprowadzić do degradacji jakości obsługi określonych aplikacji.** Realizowane jest ono poprzez kontrolę ruchu na styku użytkownik-sieć.

Z kolei **sterowanie reakcyjne ma doprowadzić do szybkiego rozładowania stanu przeciążenia sieci, rozumianego jako przekroczenie dostępnej przepustowości sieci.** Wiąże się ono z wykorzystaniem informacji zwrotnej o stanie sieci do zmiany wybranych parametrów ruchowych źródeł.

Należy przy tym podkreślić, że w zależności od typu realizowanej aplikacji odmienne są profile ruchowe źródeł, a tym samym ich „podatność” na sterowanie prewencyjne bądź reakcyjne. Trzema, najczęściej rozważanymi, w kontekście sieci ATM, typami źródeł ruchu są źródła mowy, sygnałów wideo oraz danych komputerowych. Przekazy danych rozmownych oraz zakodowanych sygnałów wideo są traktowane jako realizacje usług czasu rzeczywistego, wymagające ścisłych gwarancji odnośnie dopuszczalnego opóźnienia czy też zmienności opóźnienia przekazu komórek. Powyższe parametry odgrywają znacznie mniejszą rolę w przypadku przekazu danych komputerowych. Aplikacje typu poczta elektroniczna, WWW, czy przekaz zbiorów nie wymagają bowiem ich realizacji w czasie rzeczywistym. Istotnym parametrem jakościowym QoS staje się wówczas częstość błędów (w tym strat komórek) w procesie transmisji.

O ile więc aplikacje związane z interaktywnym przekazem mowy i obrazu nie dopuszczają praktycznie żadnej „ingerencji” sieci w zmianę parametrów ruchowych źródła, w tym wpływania sieci na szybkość nadawania komórek, to w przypadku źródeł „komputerowych” możemy stosunkowo prosto i elastycznie dostosowywać szybkość przekazu do aktualnego stanu sieci (por. np. możliwości oferowane przez protokół transportowy TCP).

*Zapewnienie określonej jakości realizacji różnych aplikacji sieciowych może być osiągnięte poprzez implementację w sieci ATM szeregu funkcji i mechanizmów zarządzania ruchem.* W szczególności są to:

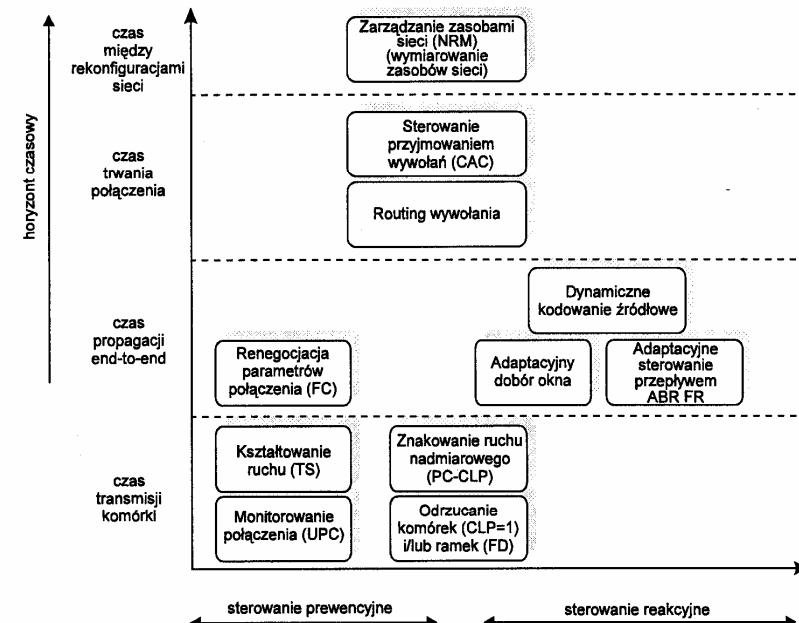
- **funkcja sterowania przyjmowaniem wywołań CAC** (ang. *Call/Connection Admission Control*), definiowana jako zespół działań mających na celu podjęcie decyzji o przyjęciu/odrzuceniu nowego wywołania, a w przypadku jego przyjęcia - przydzielenie odpowiednich zasobów sieci do realizacji połączenia;
- **funkcja monitorowania połączenia UPC** (ang. *Usage Parameter Control*), związana z procedurą sprawdzania zgodności deklaracji użytkownika z generowanym przez niego ruchem rzeczywistym. UPC może być realizowana przez algorytm GCRA (ang. *Generic Cell Rate Algorithm*), sprawdzania zgodności komórek, pozwalający na odrzucanie bądź odpowiednie znakowanie ruchu nadmiarowego, generowanego przez użytkownika, przed wprowadzeniem tego ruchu do sieci;

- **funkcja kontroli priorytetu PC** (ang. *Priority Control*), która w warunkach przeciążenia sieci, decyduje o usunięciu z sieci komórek z ustalonym bitem CLP (ang. *Cell Loss Priority*), tj. komórek o niższym priorytecie. Mechanizm kontroli bitu CLP może być także wykorzystywany przez funkcję UPC;
- **funkcja zarządzania zasobami sieci NRM** (ang. *Network Resource Management*), odpowiadająca za podział zasobów sieciowych pomiędzy poszczególne odizolowane logicznie połączenia z uwzględnieniem rodzajów usług; wykorzystuje ona koncepcję ścieżek i kanałów wirtualnych;
- **funkcja kontroli parametrów sieci NPC** (ang. *Network Parameter Control*), kontrolująca intensywność strumienia komórek na styku sieć-sieć;
- **funkcja kształtuowania ruchu TS** (ang. *Traffic Shaping*) pozwalająca wpływać na charakterystykę ruchu generowanego przez użytkownika, w celu dopasowania tej charakterystyki do deklaracji złożonej w fazie zestawiania połączenia;
- **funkcja odrzucania ramek FD** (ang. *Frame Discard*) umożliwiająca odrzucanie całych ramek w przypadku przeciążenia sieci i chroniącą tym samym pozostałe ramki przed skutkami powstającego w sieci przeciążenia;
- **mechanizm sterowania przepływem ze sprzężeniem zwotnym FC** (ang. *Feedback Control*), definiowany jako zbiór działań podejmowanych przez sieć i adresata danych, w celu wpłynięcia na szybkość generowania komórek przez źródło (w zależności od stanu sieci). Mechanizm ten wykorzystuje tzw. powiadomienie w przód - bit EFCI (ang. *Explicit Forward Congestion Indicator*) w nagłówku komórki, do poinformowania źródła o przeciążeniu w sieci;
- **mechanizm sterowania przepływem komórek dla źródeł ABR** (ang. *ABR Flow Control*) określający zasady sterowania szybkością generowania komórek przez źródło ABR. Mechanizm ten może wykorzystywać metodę sterowania FC.

Działania prewencyjne i reakcyjne podejmowane w sieci ATM w różnym horyzoncie czasowym ilustruje rysunek 7.8.

**Prewencyjna metoda sterowania ruchem związana jest przy tym z zawartiem przez użytkownika i sieć ATM tzw. kontraktu ruchowego.** Oznacza to, że w momencie inicjowania połączenia użytkownik określa parametry ruchowe źródła oraz pożądane parametry jakościowe połączenia. Na ich podstawie funkcja CAC podejmuje decyzję o przyjęciu bądź odrzuceniu wywołania do obsługi, w zależności od stanu zasobów sieci. Realizacja algorytmu decyzyjnego CAC zależy od typu stosowanej w sieci multipleksacji statystycznej. Wyróżnia się dwie koncepcje, mogące znaleźć zastosowanie w metodzie prewencyjnej. Zgodnie z pierwszą dopuszcza się obciążenie sumaryczne, generowane przez źródła, tylko nieznacznie

przekraczające pojemność łączysk transmisyjnych. W drugiej koncepcji możliwość tego przekroczenia jest znacznie większa.



Rys. 7.8. Ilustracja działań prewencyjnych i reakcyjnych związanych ze sterowaniem ruchem w sieci ATM

Przyjęcie wywołania do obsługi narzuca na obie strony „kontraktu” konieczność przestrzegania poprawności jego realizacji. Ruch generowany przez użytkownika podlega monitorowaniu przez funkcję UPC. W przypadku generacji strumienia danych o parametrach niezgodnych z kontraktem UPC dokonuje znakowania pewnych komórek i ich ewentualnego odrzucania, tak by nie spowodować pogorszenia jakości innych „zakontraktowanych” połączeń. Z kolei użytkownik, w celu zapewnienia zgodności jego parametrów rzeczywistych z deklarowanymi w kontraktie, może opcjonalnie dokonywać kształtuowania charakterystyk ruchowych źródła (funkcja TS).

Należy podkreślić, że w sieciach ATM z uwagi na ich znaczną bezwładność, wyrażającą się dużą wartością iloczynu obciążenia i czasu propagacji, sterowanie ruchem oparte na metodzie sprzężenia zwrotnego, stosowane w większości sieci pakietowych jest, w odniesieniu do aplikacji czasu rzeczywistego, całkowicie nieprzydatne. Jedynym skutecznym rozwiązaniem dla tych aplikacji jest zatem metoda

prewencyjna. Metoda ta wymaga zdefiniowania parametrów nazywanych deskryptorami ruchu, które jednoznacznie określają charakterystyki ruchu generowanego przez źródło. Są to zarówno parametry probabilistyczne jak i deterministyczne. Do pierwszych zalicza się wartość średniej intensywności ruchu, krótkookresową wariancję intensywności ruchu oraz tzw. indeks dyspersji dla zgłoszeń. Do drugiej grupy zaliczamy parametry zdefiniowane w oparciu o tzw. algorytm „cieknącego wiadra” (ang. *Leaky Bucket*). Parametry tego typu stały się podstawą propozycji przyjętych przez ATM Forum.

Dotychczas zdefiniowano następujące deskryptory ruchu wykorzystywane w metodzie prewencyjnej:

- wartość maksymalną szybkości generowania komórek PCR (ang. *Peak Cell Rate*) - definiowaną jako odwrotność minimalnego odstępu czasu między kolejnymi komórkami generowanymi przez źródło;
- graniczną wartość średniej szybkości transmisji komórek SCR (ang. *Sustainable Cell Rate*);
- maksymalny rozmiar paczki komórek MBS (ang. *Maximum Burst Size*) - określany w przypadku, gdy źródło transmituje komórki z szybkością równą SCR.

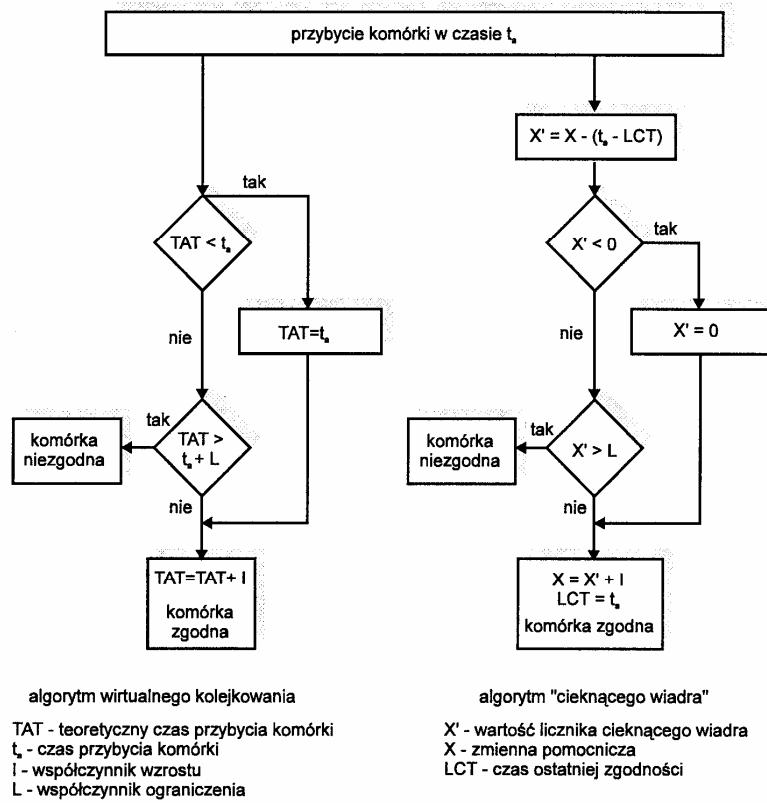
Wielkości te stanowią podzbiór parametrów ruchowych opisujących w sposób jednoznaczny charakterystykę ruchową źródła. Deskryptor źródła jest z kolei elementem deskryptora połączenia, który zawiera dodatkowo definicję tolerancji zmienności opóźnienia oraz definicję zgodności komórek dostarczanych przez źródło z warunkami kontraktu. Tolerancja zmienności opóźnienia CDV (ang. *Peak-to-peak Cell Delay Variation*) określa dopuszczalny stopień zaburzenia pierwotnego strumienia komórek np. przez funkcje układu stykowego UNI (ang. *User Network Interface*).

Kontrakt ruchowy, oprócz deskryptora połączenia, obejmuje również żądane wartości parametrów określających jakość obsługi QoS (ang. *Quality of Service Parameters*), wśród których najważniejsze to:

1. maksymalne opóźnienie przesłania komórki przez sieć MaxCTD (ang. *Maximum Cell Transfer Delay*), tj. opóźnienie mierzone od chwili rozpoczęcia transmisji pierwszego bitu komórki na wejściu sieci do chwili zakończenia odbioru ostatniego bitu komórki na wyjściu sieci, dla danego połączenia;
2. zmienność opóźnienia w przekazie komórek CDV (ang. *Peak-to-peak Cell Delay Variation*), gdzie określenie „peak-to-peak” odnosi się do różnicy pomiędzy największą i najmniejszą wartością CTD opóźnienia; najmniejsza wartość jest przy tym równa stałemu opóźnieniu (identycznemu dla każdej komórki wysłanej w czasie trwania połączenia);
3. prawdopodobieństwo CLR straty komórki (ang. *Cell Loss Ratio*), które określa się następująco:

$$\text{CLR} = \frac{\text{liczba straconych komórek}}{\text{liczba wysłanych komórek}}$$

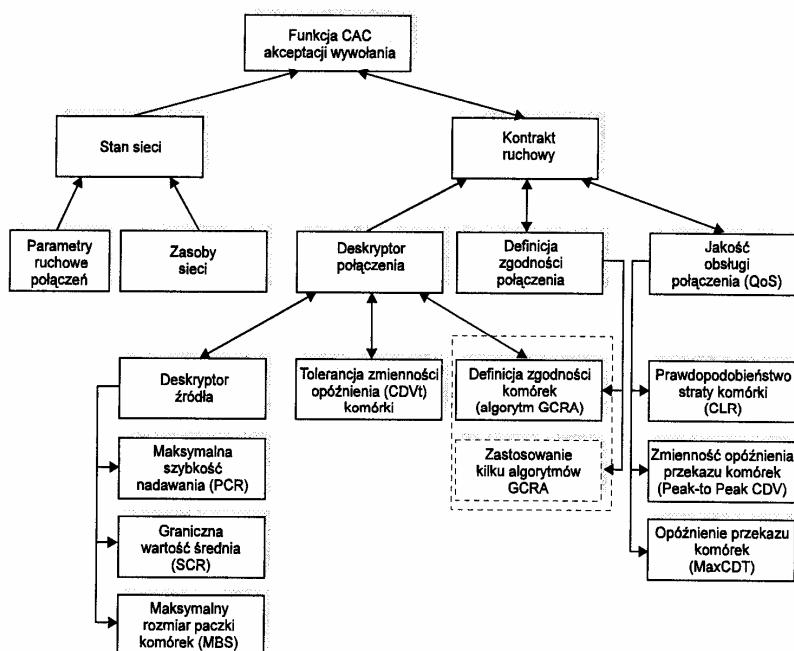
Do badania zgodności napływu komórek generowanych przez źródło z parametrami zadeklarowanymi w kontrakcie zaproponowano algorytm GCRA. Na rysunku 7.9 przedstawiono dwie równoważne wersje tego algorytmu: algorytm wirtualnego kolejkowania (ang. *Virtual Scheduling Algorithm*) oraz algorytm „cieknącego wiadra” (ang. *Continuous-State Leaky Bucket*). W obu przypadkach wykorzystywana jest para parametrów: współczynnik wzrostu określający liczbę I jednostek wnioskowanych przez napływającą komórkę, związany z szybkością transmisji i współczynnik ograniczenia pojemnościowego L, związany z długością paczek komórek (wartości współczynników I, L ustala się w fazie początkowej algorytmu).



Rys. 7.9. Równoważne wersje algorytmu GCRA monitorowania zgodności napływu komórek

W algorytmie GCRA z wirtualnym kolejkowaniem komórka uznawana jest za niezgodną wówczas, gdy jej czas przybycia do systemu nastąpił po teoretycznym czasie TAT (ang. *Theoretical Arrival Time*) - dla pierwszej przesłanej komórki wartość TAT jest równa czasowi potrzebnemu na przebycie przez komórkę „trasy” od źródła do odbiornika - pomniejszonym o współczynnik L. W przeciwnym przypadku komórka jest kwalifikowana jako zgodna. Kolejne wartości TAT są określone przez dodanie wartości współczynnika wzrostu I do poprzedniej wartości TAT.

W przypadku algorytmu cieknącego wiadra, zgodność komórki jest określana z wykorzystaniem „naczynia-bufora” o skończonej pojemności, z którego zawartość wycieka ze stałą szybkością jednej komórki na jednostkę czasu i powiększa się z szybkością I jednostek, z każdym przybyciem komórki (dopóki pojemność L nie jest przekroczona). Komórka, która powoduje przepełnienie „wiadra” jest klasyfikowana jako niezgodna. Mamy wówczas dwie możliwości: albo komórka jest odrzucana na wejściu sieci albo jest ona dopuszczana do sieci po uprzednim jej oznakowaniu bitem CLP (CLP=1). W tym drugim przypadku zakładamy, że komórki niezgodne nie spowodują degradacji obsługi innych połączeń i będą usuwane z sieci w przypadku wystąpienia przeciążenia.



Rys. 7.10. Procedury i parametry związane ze sterowaniem przyjmowaniem wywołań (CAC)

Zgodność danego połączenia ustalana jest przez funkcję UPC, w oparciu o powyższy algorytm GCRA, wykorzystywany do sprawdzenia zgodności jednego lub więcej parametrów ruchowych, zawartych w deskryptorze źródła, z ich rzeczywistymi wartościami. Definicja zgodności połączenia nie wymaga przy tym, aby wszystkie komórki były zgodne; wystarczy by liczba komórek niezgodnych nie przekroczyła zadanego progu.

Wpływ różnorodnych parametrów źródła i sieci, a także mechanizmów zgodności kontraktu na proces decyzyjny realizowany przez funkcję CAC ilustruje rysunek 7.10.

Prewencyjna metoda sterowania ruchem wraz ze swymi mechanizmami znakowania i usuwania komórek nadmiarowych, czy też kształtuowania charakterystyk źródła, skuteczna w przypadku aplikacji czasu rzeczywistego typu mowa, wideo, okazuje się być niefektywna przy przekazie danych komputerowych. Większość źródeł komputerowych charakteryzuje się bowiem nierytmiczną w przekazie danych, a tym samym dużą nieprzewidywalnością charakterystyk generowanego ruchu.

Skloniło to ATM Forum do opracowania specyficznej kategorii usług sieciowych ABR (ang. Available Bit Rate), o której mowa będzie w paragrafie 7.3.4, oraz generującymi te usługi źródłem typu ABR.

W przypadku usługi ABR połączenia „konkurują” ze sobą o dostępną pojemność, tj. niewykorzystawaną przez połączenia wymagające obsługi w czasie rzeczywistym - połączenia CBR (ang. Constant Bit Rate) bądź VBR (ang. Variable Bit Rate). Źródła ABR uzyskują dostęp do łączka tylko wtedy gdy nie ma komórek należących do połączeń CBR i VBR, tj. połączeń o wyższym priorytecie czasowym. W praktyce oznacza to, że w węzłach sieci ATM tworzone są dwa rodzaje buforów dla ruchu z wysokimi gwarancjami obsługi i ruchu obsługiwanej zgodnie z zasadą „best effort”. Tym samym ruch ABR (bądź inne nie uprzywilejowane typy ruchu) są przeźroczyste dla źródeł CBR i VBR, nie wpływając w żaden sposób na pogorszenie jakości ich obsługi. Proponowane są przy tym dwie metody dopasowania szybkości:

- Pierwsza z nich nosi nazwę metody EFCI (ang. *Explicit Forward Congestion Notification*). EFCI jest przy tym znacznikiem komórki wpisywanym w nagłówek w momencie stwierdzenia, że łączka jest przeciążone. Jeśli stacja odbierająca komórkę stwierdzi obecność takiego znacznika, to generuje specjalną informację i wysyła ją zwrotnie do stacji nadawczej. Stacja transmitująca komórki do sieci wie wtedy, że musi ograniczyć szybkość realizowanego przez nią przekazu danych. Nie wie jednak, o ile ma zmniejszyć szybkość wysyłania komórek. Dlatego też cykl taki może się powtarzać dwu lub trzykrotnie, zanim stan przeciążenia łączka komórkami zostanie likwidowany.
- Drugie rozwiązanie polega na tym, że węzeł sieci odbierający komórki może wysłać do stacji nadającej sygnał ER (ang. *Explicit Rate*), który definiuje już dokładnie, z jaką maksymalną szybkością może nadawać

źródło. ER likwiduje zjawisko przeciążenia sieci komórkami dużo szybciej niż EFCI, ponieważ stacja generująca ruch komórek w sieci jest powiadomiana o zjawisku przeciążenia niemal natychmiast, bez zbędnej zwłoki (powodowanej koniecznością kilkukrotnej wymiany informacji między stacją odbierającą komórki, a stacją wysyłającą, jak to ma miejsce w przypadku stosowania algorytmu EFCI). Aby jednak system ER pracował szybko, musi opierać się na rozwiązańach sprzętowych, a nie programowych. Sama specyfikacja usługi ABR nie definiuje dokładnie, w jaki sposób powinien pracować system ER. Firmy świadczące usługi telekomunikacyjne są zainteresowane wprowadzeniem usługi ABR w życie, gdyż pozwala ona w elastyczny sposób zarządzać pasmem przenoszenia danych oferowanym przez łącze i co za tym idzie - obniżać koszty przekazu danych.

Ważniejszymi parametrami charakteryzującymi jakość obsługi ruchu, zarówno ABR, jak i VBR i CBR poza wymienionymi wcześniej (maxCTD, Peak-to-peak CDV, CLR), są:

- prawdopodobieństwo CER straty komórki (ang. *Cell Error Ratio*), wynikające z błędów transmisji, wyrażone jako:

$$\text{CER} = \frac{\text{liczba błędnych komórek}}{\text{liczba dobrze przesłanych komórek} + \text{liczba błędnych komórek}},$$

- prawdopodobieństwo CIR „wtrącenia” komórki (ang. *Cell Injection Ratio*) do innego połączenia wirtualnego na skutek przekłamania identyfikatora VCI/VPI, definiowane jako:

$$\text{CIR} = \frac{\text{liczba komórek "wtrąconych"}}{\text{liczba komórek przesłanych}},$$

- prawdopodobieństwo przekłamania bloku komórek SECBR (ang. *Severely Errored Cell Block Ratio*), określone jako:

$$\text{SECBR} = \frac{\text{liczba bloków znacznie przekłamanych}}{\text{liczba wysłanych bloków}},$$

gdzie blok komórek jest sekwencją N komórek wysłanych w danym połączeniu. Blok taki jest uznawany za znacznie przekłamany, jeżeli łącznie więcej niż M komórek zostało przekłamanych lub straconych, spośród N komórek w danym bloku ( $M < N$ ).

- intensywność źle skomutowanych komórek CMR (ang. *Cell Misinsertion Rate*), wyrażona jako:

$$\text{CMR} = \frac{\text{liczba źle skomutowanych komórek}}{\text{przedział czasu}}.$$

Ważnym problemem w sieci B-ISDN ATM jest zarządzanie połączeniami typu ścieżka wirtualna VPC i kanał wirtualny VCC. Zarządzanie połączeniami wirtualnymi typu VCC i VPC polega między innymi na: monitorowaniu jakości transmisji, wykrywaniu i zawiadamianiu o awariach oraz na przeprowadzaniu różnego rodzaju testów kontrolnych. Informacje sterujące, takie jak powiadomienia o awariach, monitorowanie poprawności przesyłanych danych i żądanie wykonania testów, muszą być wymieniane pomiędzy węzłami sieci. Mechanizmy zapewniające transmisję tych informacji, na poziomie ścieżek wirtualnych VP (ang. *Virtual Path*) i kanału wirtualnego VC (ang. *Virtual Channel*), zostały zdefiniowane przez ITU-T i są opisane jako strumienie F4 (dla VPC) i F5 (dla VCC), dla każdego z połączeń. Wymiana danych w strumieniach sterujących F4 i F5 odbywa się za pomocą specjalnych komórek. Zawierają one informacje sterujące, np. informujące o poprawności przesyłanych danych. Komórki te, nazywane komórkami sterującymi i zarządzającymi OAM, są odróżniane od komórek danych poprzez inny format nagłówka. ITU-T zdefiniowało trzy typy komórek OAM:

- zarządzających sprawnością sieci;
- informujących o awariach sieci oraz
- wykorzystywanych do aktywacji i dezaktywacji różnych funkcji zarządzających.

Zadaniem komórek OAM zarządzających sprawnością sieci jest wspomaganie monitorowania jakości połączeń typu VCC i VPC oraz zarządzanie ruchem w sieci, w tym powiadamianie węzłów o przeciążeniach.

Z kolei zadaniem komórek OAM zarządzających awariami jest przekazywanie informacji o stanach alarmowych, sprawdzanie ciągłości połączeń, jak również testowanie samej sieci.

Komórki OAM - aktywacji i dezaktywacji, umożliwiają włączanie i wyłączanie funkcji wspomagających połączenia VPC/VCC.

Należy zwrócić uwagę na to, że część funkcji zarządzania siecią i sterowania ruchem może być przeniesiona z warstwy ATM do warstwy adaptacji AAL. Ma to na celu zagwarantowanie poprawności realizacji określonych aplikacji sieciowych. Trzeba też podkreślić, że nie wszystkie wymienione powyżej mechanizmy i procedury muszą być zaimplementowane i realizowane w danej sieci ATM.

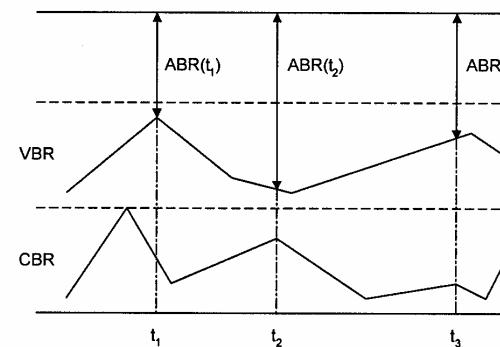
#### 7.3.4 Kategorie i klasy usług warstwy ATM

Zakłada się, że sieci B-ISDN ATM będą oferować różne typy usług. ATM Forum w swoim zaleceniu „Traffic Management v.4.0” zdefiniowało pięć podstawowych kategorii usług. Ich wprowadzenie pozwoliło na dostosowanie funkcji zarządzania ruchem takich jak routing, CAC, UPC czy też zarządzanie zasobami sieci NRM do poszczególnych typów ruchu. Dotychczas zdefiniowane kategorie usług to:

- **usługa o stałej szybkości bitowej CBR** - opracowana dla źródeł ruchu wymagających stałej szybkości transmisji w czasie trwania połączenia. W przypadku tej kategorii wartość wymaganego pasma transmisyjnego określana jest przez maksymalną szybkość przekazu PCR. Kategoria ta jest wykorzystana do emulacji łącza cyfrowego o przepływności 2.048 Mb/s. Przykładami aplikacji korzystających z tej usługi są interaktywne przekazy mowy czy też transmisje sygnałów wideo w standardzie MPEG1;
- **usługa o zmiennej szybkości bitowej VBR** - przewidziana dla źródeł ruchu generujących komórki ze zmienią ale ograniczoną maksymalną intensywnością transmisji i wymagających gwarantowanego poziomu jakości usług. Obecnie usługa ta jest podzielona na dwa typy:
  1. **rt-VBR** (ang. *Real-Time Variable Bit Rate*) - wstępnie przewidziana dla źródeł wymagających obsługi w czasie rzeczywistym, dla których są gwarantowane trzy podstawowe parametry jakości obsługi QoS: CDV, CTD oraz CLR. Wymagane pasmo transmisyjne jest obliczane na podstawie wartości parametrów PCR, SCR i MBS. Przykładami aplikacji korzystających z tego typu usługi są: przekazy sygnałów mowy, a także skompresowanych obrazów ruchomych zakodowanych w standardzie MPEG2;
  2. **nrt-VBR** (ang. *Non-Real-Time Variable Bit Rate*) - usługa przewidziana dla źródeł nie wymagających synchronizmu czasowego w przekazie informacji między źródłem, a odbiornikiem. Usługa nrt-VBR wymaga zadeklarowania przez źródło tych samych parametrów ruchowych co rt-VBR. Sieć z kolei, spośród parametrów QoS, gwarantuje jedynie prawdopodobieństwo straty komórki. Przykładami aplikacji korzystających z tej usługi mogą być: transmisje ważnych danych komputerowych, czy też szybki przekaz poczty elektronicznej;
- **usługa o niezdefiniowanej szybkości bitowej UBR** (ang. *Unspecified Bit Rate*) - przewidziana dla źródeł o niezdefiniowanej szybkości transmisji, realizujących nieregularny przekaz danych, w miarę dostępności łączka. W przypadku stosowania usługi UBR, aplikacja wysyła dane w sieć i nie interesuje się, czy i kiedy dane te dotrą do celu. Sieć z kolei postępuje zgodnie z zasadą największego wysiłku tj. „best effort”. W związku z tym, w momentach przeciążenia łączka usługami innych typów dane przesypane w ramach UBR są po prostu tracone;
- **usługa o niezdefiniowanej szybkości bitowej UBR+** przewidziana dla aplikacji dopuszczających przekaz zgodnie z zasadą „best effort” z wyłączeniem funkcji odrzucania komórek, decydującej o usunięciu z sieci komórek z ustawionym bitem CLP. Podobnie jak w usłudze UBR brak jest jakichkolwiek gwarancji dotyczących jakości obsługi. Obie kategorie usług (UBR i UBR+) zostały dopasowane do potrzeb wielu tradycyjnych sieci komputerowych LAN, np. Ethernet, Token Ring, bądź WAN, np. X.25, Frame Relay, które generują ruch typu nrt (ang. *non-real-time*) i realizują obsługę typu „best effort”. Przykładem może też być sieć Internet, w której protokół datagramowy IP może „gubić” pakiety. Zadaniem protokołu transportowego TCP, w tej sieci, jest zapewnienie integralności i niezawodności przekazu.

- **usługa o dostępnej szybkości bitowej ABR** - przewidziana dla źródeł o niezdefiniowanej szybkości transmisji, umożliwiająca użytkownikowi wykorzystanie, w danym momencie, całej dostępnej przepustowości kanału. ABR zawiera mechanizm kontroli przeciążenia sieci, który zapobiega utracie danych w momentach wzmożonego ruchu. Mechanizm ten po stwierdzeniu, że w sieci jest przeciążenie, zmusza systemy końcowe do zmniejszenia intensywności transmisji lub wręcz wstrzymania przesyłania danych. Tym samym ABR to usługa oferująca zmienne pasmo transmisyjne i nie narzucająca krytycznych wymagań czasowych. Typ ABR usług może być zatem stosowany do obsługi aplikacji nie wymagających gwarantowanego czasu dostarczenia danych do adresata, takich jak np. przekaz plików czy poczta elektroniczna. ABR gwarantuje przy tym (między innymi dzięki zastosowaniu reakcyjnej metody sterowania ruchem) ograniczony poziom strat komórek.

Innym typem usługi, zdefiniowanej jedynie przez ITU-T, jest **usługa ABT** (ang. *ATM Block Transfer*) **blokowego przekazu danych**, wykorzystująca ideę dynamicznej rezerwacji pasma przy pomocy komórek zarządzających RM (ang. *Resource Management*). Usługa ta przewidziana jest do obsługi aplikacji generujących dane w postaci bloków o różnych wymaganiach odnośnie pasma. Każda przesyłana porcja danych przedzielana jest komórkami zarządzającymi RM umożliwiającymi wynegocjowanie odpowiedniej szybkości bitowej do wartości PCR włącznie. Oprócz parametru PCR mogą być również negocjowane parametry dodatkowe jak np. minimalna gwarantowana wartość szybkości.



Rys. 7.11. Wykorzystanie przepustowości łączka przez różne rodzaje usług

Wykorzystanie przepustowości łącza przez różne rodzaje usług (i generujące je źródła) ilustruje rysunek 7.11. Zgodnie z ilustracją część przepustowości łącza jest zarezerwowana przez stacje typu CBR np. do przesyłania glosu, inna część jest przydzielona źródłom VBR np. do przesyłania skompresowanego obrazu wideo, a reszta poprzez ABR może być np. wykorzystana do obsługi poczty elektronicznej, przekazu plików i zdalnych sesji terminalowych. ABR wykorzystuje więc tę część przepustowości, która w danym momencie nie jest wykorzystywana przez inne usługi.

Kategorie usług CBR i VBR wykorzystują do sterowania ruchem metodę prewencyjną. W przypadku kategorii UBR nie stosuje się żadnej metody sterowania, zakładając, że dane generowane przez źródło UBR obsługiwane są zgodnie zasadą „best effort”, lecz bez gwarancji (jakości) ich dostarczenia przez sieć do adresata. W przypadku kategorii ABR wykorzystuje się reakcyjną metodę sterowania. Zapewnia ona ograniczenie prawdopodobieństwa strat komórek i sprawiedliwy dostęp do zasobów sieci.

Kategorie usług warstwy ATM wraz z wymaganymi parametrami, określającymi ruch generowany przez użytkownika przedstawia tabela 7.3.

Tabela 7.3. Kategorie usług warstwy ATM

	Typy usług warstwy ATM				
	CBR	rt-VBR	nrt-VBR	UBR, UBR+	ABR
Parametry ruchowe:					
PCR, CDV <sub>t</sub>	deklarowane wartości				
SCR, MBS i CDV <sub>t</sub>	n/d	deklarowane	n/d		
MCR	n/d			deklarowane	
Parametry QoS:					
Peak-to-peak CDV	deklarowane	n/d			
max. CTD	deklarowane	n/d			
CLR	deklarowane		n/d	deklarowane	
Informacje kontrolne	brak			sprzężenie zwrotne	

n/d - nie deklarowany

W sieci B-ISDN ATM zdefiniowano też kilka klas usług warstwy ATM. Są one związane z omówionymi powyżej kategoriami źródeł i usług, wynikającymi z obsługi różnych aplikacji, odmiennego sposobu przesyłania informacji, odmiennej wymaganej szerokości pasma i różnego rodzaju realizowanych połączeń. Podstawowe klasy to:

- klasa A - obejmuje ona usługi połączeniowe realizowane ze stałą szybkością transmisji - CBR, przeznaczone do zastosowań multimedialnych w czasie rzeczywistym (dźwięk, wideo, wideokonferencja);

- klasa B - obejmuje ona usługi połączeniowe związane z przesyaniem glosu i obrazów wideo ze zmienią chwilową szybkością transmisji - VBR;
- klasa C - obejmuje ona usługi połączeniowe oferowane ze zmienią chwilową szybkością transmisji i bez synchronizacji czasowej (X.25, Frame Relay, TCP/IP - ruch typu nrt-VBR i ABR);
- klasa D - obejmuje ona usługi bezpołączeniowe; do tej klasy zaliczamy usługi, w których przepływ danych odbywa się ze zmienią szybkością i nie jest wymagana synchronizacja czasowa między węzłami końcowymi (dane pochodzące z sieci LAN, MAN, WAN - ruch typu UBR).

Wymienia się także (zgodnie z klasyfikacją ITU-T) klasy X i Y, wskazując na ich przeznaczenie do przekazu plików przez sieć łączności bezpośredniej, po uzgodnieniu z aplikacją pasma przenoszenia danych i jakości usługi sieciowej (klasa X) bądź maksymalnej i średniej szybkości transmisji danych (klasa Y).

Krótką charakterystyką klas A-D zawarta jest w tabeli 7.4. Klasyfikacja ta podana została z uwzględnieniem tego, czy wymagana jest synchronizacja między terminalami i czy mamy do czynienia z połączeniowym, czy też bezpołączeniowym przekazem danych, w realizowanej aplikacji.

Tabela 7.4. Klasy i kategorie usług ATM

	Klasy i kategorie usług			
	A (CBR)	B (rt-VBR)	C (nrt-VBR/ABR)	D (UBR)
Synchronizacja	wymagana między terminalami			nie wymagana
Szybkość bitowa	stała		zmienna ustalana przez źródło	zmienna ustalana przez sieć
Tryb połączenia		połączeniowy (AAL 3/4)		beopołączeniowy
Warstwa AAL	typ 1	typ 2	typ 5	typ 3/4

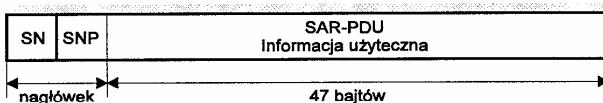
Standard ATM zapewnia podstawowy przekaz informacji w trybie połączeniowym. Oznacza to, że przed przesaniem informacji właściwej musi mieć miejsce faza zestawienia połączenia, na podstawie parametrów deklarowanych przez abonenta (typ usługi, przewidywana szybkość transmisji, docelowy adres), a po zakończeniu przekazu - jego likwidacja. Parametry zadeklarowane we wstępnej fazie mogą podlegać renegocjacji.

## 7.4 Warstwa adaptacyjna ATM

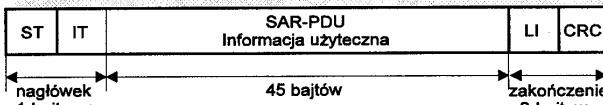
Warstwa adaptacyjna AAL (ang. *ATM Adaptation Layer*), „przekształca” pakiety napływające z wyższych warstw do postaci komórek ATM. Jest ona zorganizowana w postaci dwóch logicznych podwarstw: podwarstwy zbieżności (konsolidacji) CS (ang. *Convergence Sublayer*) oraz podwarstwy segmentacji i odtwarzania SAR (ang. *Segmentation And Reassembly*). Podwarstwa zbieżności odbiera

dane z wyższych warstw i po ich ewentualnym uzupełnieniu o nagłówki i zakończenia przekazuje do podwarstwy SAR. Ta z kolei odpowiada za fragmentację danych na bloki 48-mio bajtowe.

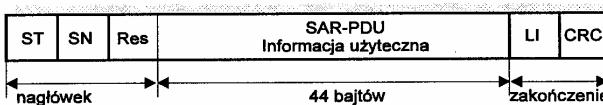
#### 7.4.1 Typy protokołów warstwy AAL



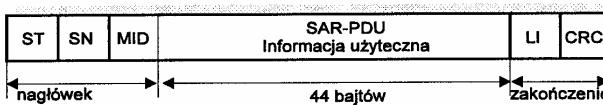
a) Struktura danych podwarstwy SAR dla AAL typ 1



b) Struktura danych podwarstwy SAR dla AAL typ 2



c) Struktura danych podwarstwy SAR dla AAL typ 3



d) Struktura danych podwarstwy SAR dla AAL typ 4

SN (Sequence Number - 4 bity) - numer kolejny

SNP (Sequence Number Protection - 4 bity) - ochrona SN

IT (Information Type - 4 bity) - typ informacji

LI (Length Indicator - 6 bitów) - wskaźnik, długości

CRC (Cyclic-Redundancy-Check - 10 bitów) - ciąg kontrolny kodu cyklicznego

ST (Segment Type - 2 bity) typ segmentu

Res (Reserved - 10 bitów) - rezerwa

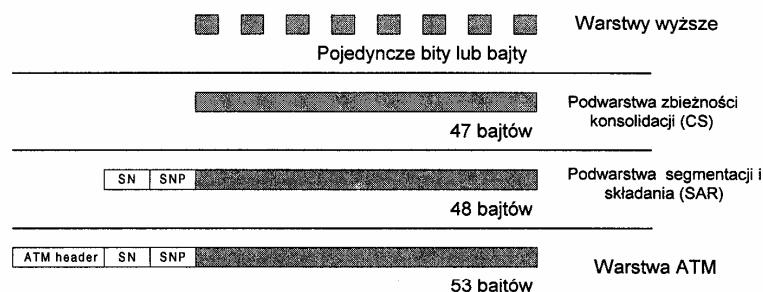
MID (Multiplexing IDentity - 10 bitów) - identyfikator multipleksowania

Rys. 7.12. Struktura danych podwarstwy SAR dla protokołów typów 1-4 warstwy AAL

W celu zapewnienia właściwej obsługi różnych rodzajów źródeł zdefiniowano 5 różnych protokołów warstwy AAL. Protokół AAL typ 1 wspomaga klasę A usług i jest wykorzystywany do realizacji np. połączeń telefonicznych wymagających stałej szybkości transmisji. Jest to typowy protokół zorientowany połączeniowo. Protokół AAL typ 2 podtrzymuje klasę B usług. Wykorzystywany jest on do przesyłania informacji o zmiennej szybkości transmisji lecz o bardzo wysokim rygorze czasowym. Klasę C usług ma podtrzymywać protokół AAL typ 5. Wykorzystywany jest on do transmisji o zmiennej szybkości, bez specjalnych wymogów

#### 7.4 Warstwa adaptacyjna ATM

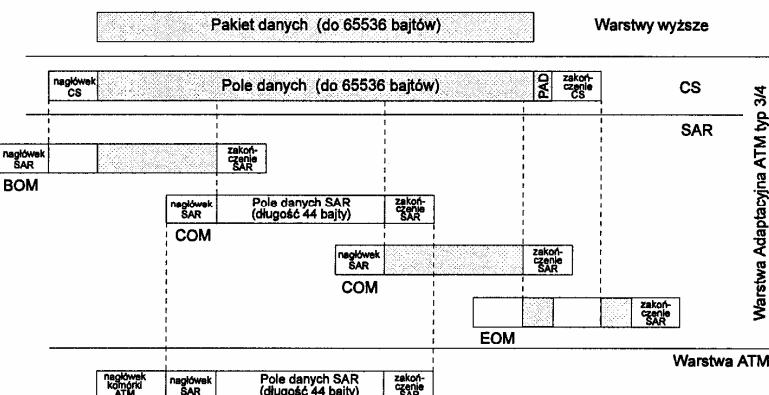
czasowych (nie jest wymagana synchroniczna praca pomiędzy nadajnikiem a odbiorikiem). AAL typ 5 przeznaczony jest do obsługi ruchu o dużej szybkości transmisji, pochodzącego np. z sieci TCP/IP i Frame Relay. Z kolei klasę D usług podtrzymują protokoły AAL typów 3/4. Ten typ protokołów może być wykorzystany do transmisji o zmiennej szybkości i bez specjalnych wymagań czasowych, tj. głównie do obsługi ruchu UBR. Ilustrację związków pomiędzy protokołami warstwy AAL, a wspomaganymi przez nie przykładowymi aplikacjami pokazuje tabela 7.5. Z kolei rysunek 7.12 pokazuje formaty protokolarnych jednostek danych (PDU) warstwy SAR dla 4 typów protokołów AAL. Zasady segmentacji/scalania komórek ATM w warstwie adaptacji dla typów 1, 3/4 i 5 protokołów warstwy AAL, ilustrują rysunki 7.13, 7.14 i 7.15.



SN (Sequence Number) - numer kolejny

SNP (Sequence Number Protection) - ochrona SN

Rys. 7.13. Tworzenie komórek w przypadku AAL1

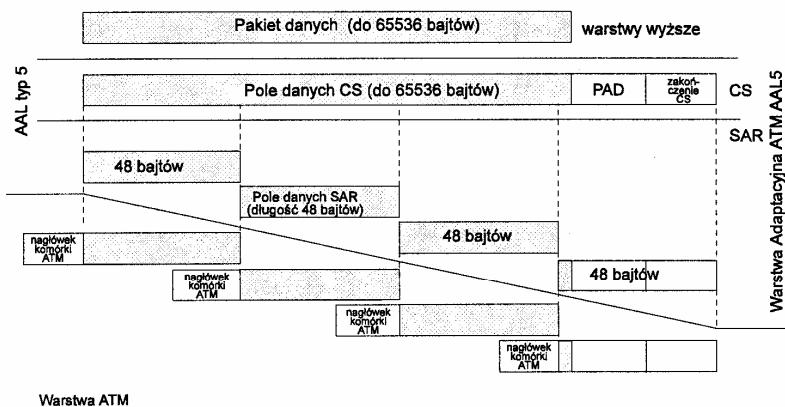


BOM (Begin Of Message) - początek wiadomości

COM (Continuation Of Message) - kontynuacja wiadomości

EOM (End Of Message) - koniec wiadomości

Rys. 7.14. Procedury segmentacji/scalania pakietu zgodnie z AAL3/4



Rys. 7.15. Procedury segmentacji/scalania pakietu danych zgodnie z AAL5

Tabela 7.5. Powiązania klas protokołów AAL z przykładowymi aplikacjami

Wyższe warstwy modelu ISO/OSI (przykładowe aplikacje):			
AAL 1	AAL 2	AAL 5	AAL 3/4
telefonia (mowa), emulacja łącza, telekonferencje	HDTV (obrazy), wideokonferencje	Frame Relay, SMDS, TCP/IP, X.25: ważna transmisja danych, szybka poczta elektroniczna	LAN, MAN: transmisja danych, przekaz plików

## 7.5 Połączenia w sieci ATM

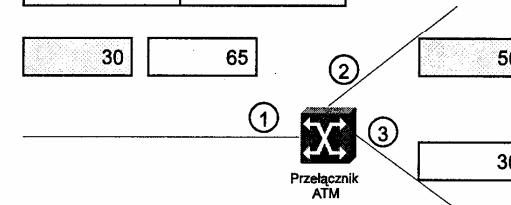
ATM jest protokołem połączniowym z komutacją pakietów. Oznacza to, że przed rozpoczęciem transmisji danych musi zostać utworzone wirtualne połączenie pomiędzy nadawcą i odbiorcą, a przesyłane dane dzielone są na fragmenty przekazywane w kolejnych komórkach. Podstawowa operacja wykonywana przez komutator ATM jest bardzo prosta. Składają się na nią następujące kroki:

- odbiór komórki przez jeden z portów wejściowych komutatora;
- odszukanie identyfikatora VPI/VCI odebranej komórki w lokalnej tablicy translacji w celu określenia portu (lub portów) wyjściowego oraz nowej wartości VPI/VCI dla danego połączenia;
- retransmisji odebranej komórki przez odpowiedni port z nowymi wartościami VPI/VCI.

Opisane powyżej czynności ilustruje rysunek 7.16. Tak prosty algorytm działania możliwy jest do zrealizowania jedynie dzięki wcześniejszemu stworzeniu lokalnej tablicy translacji, do czego wykorzystywane są mechanizmy uruchamiane przed rozpoczęciem transmisji danych. Przy tworzeniu i modyfikacji tablic wyróżnia

się dwa podstawowe, ze względu na przebieg procesu zestawiania, typy połączeń ATM:

Wejście	Wyjście
Port VPI/VCI	Port VPI/VCI
1 30	2 50
2 50	1 30
1 65	3 30
3 30	1 65



Rys. 7.16. Ilustracja operacji przyporządkowania identyfikatorów VPI/VCI w przełączniku (komutatorze) ATM

- PVC (ang. *Permanent Virtual Connection*); stałe połączenia wirtualne. Są to połączenia zestawiane przez pewien mechanizm zewnętrzny w stosunku do sieci ATM. Polegają one na przydzieleniu stałych wartości identyfikatorów VPI/VCI w zbiorze komutatorów na drodze pomiędzy dwoma wybranymi komutatorami ATM. System sygnalizacji oferowany przez ATM może ułatwiać zestawianie tego typu połączeń, jednak z definicji, zawsze wymagają one pewnej manualnej ingerencji administratora sieci.
- SVC (ang. *Switched Virtual Connection*); przełączane połączenia wirtualne. Są to połączenia zestawiane automatycznie przez protokół sygnalizacji ATM. Nie wymagają one manualnej interakcji, tak jak jest to wymagane w przypadku PVC i jako takie są dużo częściej stosowane. Wszystkie protokoły warstw wyższych operujące na ATM używają głównie tego rodzaju połączeń.

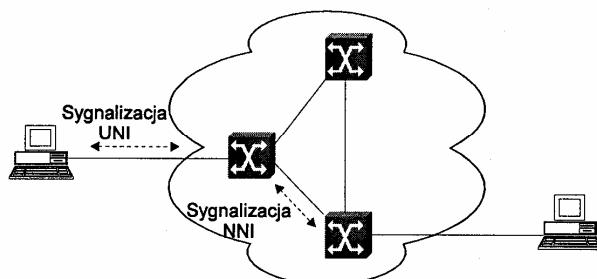
Proces tworzenia połączenia SVC, a w szczególności określenie drogi, którą przebywa żądanie zestawienia połączenia ATM (ang. *ATM signaling request*) oraz przesypane w jego obrębie komórki kontrolowanej jest przez odpowiednie protokoły routingu.

### 7.5.1 Routing w sieciach ATM

ATM Forum prowadzi prace nad protokołami routingu w dwóch płaszczyznach. Pierwsza obejmuje protokoły routingu dla publicznych sieci ATM, używających adresów w formacie E.164, druga z kolei protokoły pracujące w sieciach prywatnych ATM, czyli wykorzystujących adresowanie formatu NSAP.

Sieci publiczne ATM mają być łączone przy wykorzystaniu stosu protokołu NNI, opartego na protokołach ITU-T B-ISUP oraz ITU-T MTP Level 3. Prace standaryzacyjne w tym kierunku prowadzone są przez wchodząą w skład ATM Forum, grupę roboczą Broadband Inter-Carrier Interface (B-ICI) Group oraz inne międzynarodowe organizacje standaryzujące. Na dzień dzisiejszy nie powstał jednak jeszcze spójny standard protokołu dla sieci publicznych, dlatego też w rozdziale tym zajmiemy się głównie prywatnymi sieciami ATM oraz wykorzystywanym w nich protokołem P-NNI (ang. *Private NNI protocol*).

**Protokół P-NNI składa się z dwóch komponentów. Pierwszym jest protokół sygnalizacji P-NNI (ang. *P-NNI signaling protocol*). Zapewnia on wymianę informacji przez NNI pomiędzy komutatorami ATM oraz dokonuje odwzorowania sygnałów UNI na NNI w komutatorze źródłowym (ang. *ingress switch*) i sygnałów NNI na UNI w komutatorze docelowym (ang. *egress switch*), zgodnie z ilustracją zawartą na rysunku 7.17. Dane protokołu, jak żądania zestawienia połączenia, przesyłane są w postaci elementów informacyjnych IE (ang. *Information Elements*) w komórkach ATM o VCI=5.**



Rys. 7.17. Sygnalizacja UNI i NNI

**Drugim komponentem protokołu P-NNI jest protokół routingu połączeń wirtualnych** (ang. VCRP - *Virtual Circuit Routing Protocol*). Dysponując informacjami o stanie sieci, ma on za zadanie znalezienie drogi do adresata, będącej jednocześnie trasą wymiany przesyłanych w trakcie połączenia komórek. Protokół ten wykorzystuje techniki znane z wcześniejszych rozwiązań tego typu, lecz za względu na stopień skalowalności sieci ATM oraz wymóg zapewnienia rzeczywistej obsługi QoS, jest znacznie bardziej złożony.

Realizowana w sieciach ATM jakość obsługi (QoS) wymusza istnienie wielu metryk, który to fakt implikuje z kolei istnienie wielu atrybutów łączy fizycznych oraz węzłów sieci. Dotychczas zdefiniowano następujące metryki:

- maksymalne opóźnianie transmisji komórki (ang. MCTD *Maximum CTD*), dla danej klasy ruchu;
- maksymalną wariancję opóźnienia komórki (ang. MCDV *Maximum CDV*), dla danej klasy ruchu;

- maksymalną stopę utraty komórek (ang. MCLR *Maximum CLR*) dla CLP=0, dla klas CBR i VBR;
- wagę administracyjną (ang. *Administrative Weight*), ustawianą przez administratora i mającą wskazywać na pożądany stopień wykorzystania łącza oraz następujące atrybuty łączy:
  - dostępne pasmo przepustowe (ang. ACR *Available Cell Rate*), dla danej klasy ruchu;
  - margines przydziału pasma (ang. CRM *Cell Rate Margin*) określający różnicę pomiędzy podtrzymywana szybkością transmisji, a rzeczywiście przydzielonym pasmem dla danej klasy ruchu;
  - współczynnik niezgodności (ang. VF *Variance Factor*), czyli wartość CRM dla danej klasy ruchu znormalizowaną względem sumy CRM dla wszystkich klas.

W najprostszym ujęciu **protokół routingu VCRP ma zapewnić znalezienie ścieżki od źródła do punktu docelowego, która sprosta wymaganiom jakości obsługi QoS oraz dla której prawdopodobieństwo akceptacji przez wszystkie funkcje CAC w komutatorach pośrednich jest największe**. W tym celu wykorzystywany jest protokół badania stanu i topologii sieci (ang. *Topology State Routing Protocol*), pozwalający węzłom na rozsyłanie i gromadzenie opisanych powyżej informacji. Dane te wymieniane są jako PTSP (ang. *P-NNI Topology State Packets*) i zawierają informacje typ-wymiar-wartość (ang. TLV *Type-Length-Value*) zakodowane w postaci elementów stanu topologii PTSE (ang. *P-NNI Topology State Elements*).

**Komutator otrzymujący żądanie nawiązania połączenia dysponuje więc pewną estymatą stanu sieci. Pozwala mu ona na określenie całej ścieżki, po której przebiegać będzie połączenie, aż do komutatora docelowego. Protokół P-NNI jest więc protokołem wykorzystującym technikę routingu źródłowego** (ang. *source routing*). Wybranie tej techniki routingu w miejsce techniki hop-by-hop wynika z kilku przyczyn:

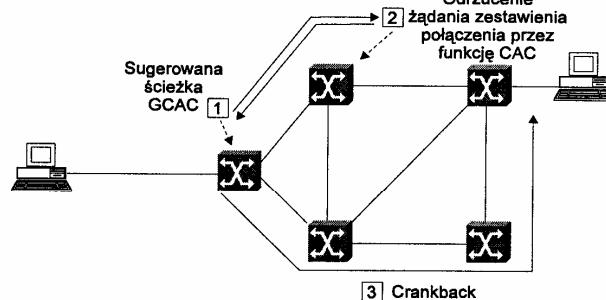
- łatwiejsza realizacja rzeczywistej QoS;
- brak potrzeby definiowania dodatkowego protokołu unikania zapętleń;
- algorytm znajdowania ścieżki wykonywany jest jednokrotnie, podczas gdy pozostałe komutatory tylko wykonują własną funkcję CAC, akceptując bądź odrzucając żądanie zestawienia połączenia;
- łatwość realizacji mechanizmu Crankback.

Tego typu rozwiązanie implikuje także brak potrzeby standaryzacji algorytmu doboru ścieżki, pozostawiając jego wybór i implementację w gestii producenta sprzętu. W rzeczywistości, znaleziona ścieżka jest tylko próbą odgadnięcia rozwiązania optymalnego. Jest to wynikiem szybko zmieniającego się stanu sieci oraz faktu, iż algorytm CAC zaimplementowany w komutatorach pośrednich, podobnie jak algorytm doboru ścieżki, nie podlega standaryzacji. Aby zapewnić odpowiednio niskie prawdopodobieństwo pomyłki protokół P-NNI definiuje standardową funkcję CAC - GCAC (ang. *Generic CAC*). Funkcja ta, wykorzystując

pewien minimalny zbiór opisanych powyżej atrybutów łączy i metryk, pozwala na określenie przewidywanego zachowania funkcji CAC innego komutatora. Została ona zaprojektowana głównie dla połączeń CBR i VBR. Działanie funkcji dla połączeń UBR ogranicza się jedynie do sprawdzenia, czy dany węzeł sieci obsługuje ten typ ruchu. Dla połączeń ABR dodatkowo sprawdzane jest, czy atrybut ACR przewyższa minimalną dopuszczalną szybkość transmisji MCR (ang. *Minimum Cell Rate*).

Używając funkcji GCAC komutator, otrzymujący żądanie zestawienia połączenia, które zostało zaakceptowane przez jego funkcję CAC, wykonuje następujące kroki:

- 1) analiza metryk nieaddytywnych - ze zbioru wszystkich łącz w sieci odrzucane są łącz, które nie mogą zapewnić wymaganych przez żądanie wartości ACR oraz CLR;
- 2) znajdowanie najkrótszej ścieżki - na pozostałym zbiorze łącz wykonywany jest algorytm najkrótszej ścieżki, w celu wyłonienia jednej lub wielu ścieżek do punktu przeznaczenia;
- 3) analiza metryk addytywnych - ze zbioru ścieżek usuwane są ścieżki o sumarycznej wartości CTD przekraczającej wartość wymaganą w żądaniu;
- 4) wybór jednej ścieżki - z otrzymanego zbioru akceptowalnych ścieżek wybierana jest jedna (niekoniecznie najlepsza z możliwych; komutator może np. uruchomić mechanizm analizy i równoważenia obciążenia);
- 5) transmisja wyników - komutator konstruuje strukturę zawierającą opis ścieżki DTL (ang. *Designated Transit List*) oraz dodaje ją do żądania; następnie, przy wykorzystaniu protokołu sygnalizacji P-NNI, żądanie przekazywane jest do kolejnych komutatorów na wyznaczonej ścieżce.

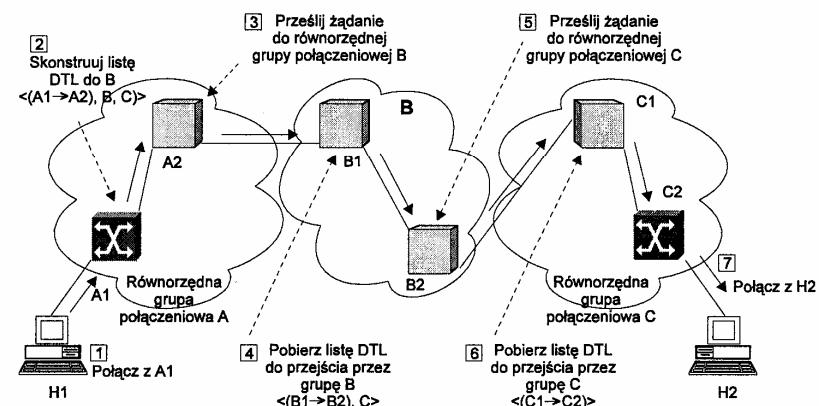


Rys. 7.18. Proces zestawiania połączenia z wykorzystaniem mechanizmu Crankback

Przechodzące przez kolejne komutatory żądanie zestawienia połączenia musi zostać zaakceptowane przez ich lokalne funkcje CAC. W przypadku odrzucenia żądania uruchamiany jest mechanizm Cranback. Polega on na cofnięciu żądania, wzdłuż ustalonej ścieżki, do najbliższego komutatora realizującego funkcję konstrukcji DTL. Komutator ten podejmuje działania analogiczne do opisanych

powyżej, jednak w oparciu o zaktualizowany stan sieci. Operację tę ilustruje rysunek 7.18. Proces zestawiania połączenia kończy się, gdy ostatni z komutatorów na liście DTL zaakceptuje żądanie wykonując lokalną funkcję CAC lub gdy po kilkukrotnej próbie nie udało się zrealizować połączenia.

Przedstawiony powyżej opis jest jedynie zarysem działania protokołu P-NNI. Nie uwzględniono w nim bardziej szczegółowych aspektów, które uwidaczniają się szczególnie w przypadku rozległych sieci ATM. Do problemów takich zalicza się np.: wzrost długości list DTL oraz trudności z gromadzeniem i przechowywaniem informacji o stanie sieci. Tutaj nadmienimy jedynie, iż z tego typu niedogodnościami protokół P-NNI radzi sobie dokonując dekompozycji sieci, a więc traktując pewne jej fragmenty jako pojedyncze łącz lub systemy komutujące. Fragmenty takie nazywane są równorzędnymi grupami połączeniowymi (ang. *peer group*). Grupy takie połączone są poprzez wydzielone komutatory graniczne (ang. *border node*), które w momencie otrzymania żądania zestawienia połączenia realizują odpowiedni routing w obrębie swojej grupy. Mechanizm ten został zilustrowany na rys. 7.19.



Rys. 7.19. Proces zestawiania połączenia z wykorzystaniem list DTL

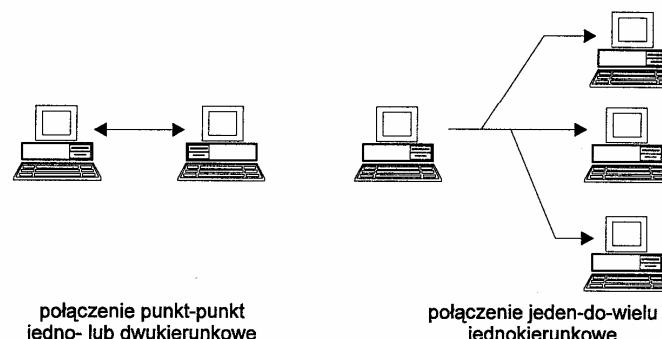
## 7.5.2 Rodzaje połączeń w sieci ATM

Sieć ATM może realizować następujące rodzaje połączeń pomiędzy użytkownikami końcowymi:

- połączenia punkt-punkt (ang. *point-to-point connection*) - łączące dwa systemy końcowe. Mogą one być jedno- (ang. *uni-*) lub dwukierunkowe (ang. *bidirectional*).
- połączenia punkt-wielopunkt (jeden do wielu) (ang. *point-to-multipoint connection*) - łączące pojedynczy, źródłowy system końcowy, nazywany korzeniem (ang. *root node*) z wieloma docelowymi systemami końcowymi, nazywanymi liśćmi (ang. *leaves*). W przypadku takich połączeń

komutatory dokonują automatycznego powielania komórek, tak aby zapewnić odpowiednie rozgałęzienia połączenia. Połączenia takie są jednokierunkowe, umożliwiając transmisję danych od korzenia do liści, ale nie w odwrotnym kierunku.

Typy połączeń w sieci ATM przedstawiono na rysunku 7.20.

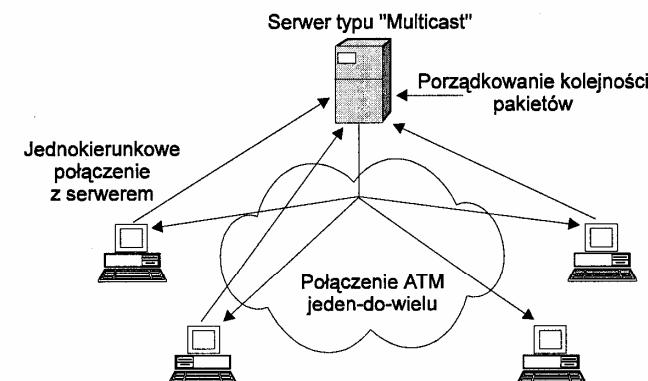


Rys. 7.20. Typy połączeń w sieci ATM

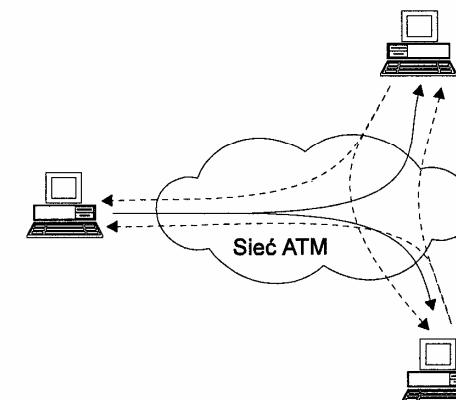
Wśród typów połączeń oferowanych przez sieć ATM brakuje połączeń multycastowych oraz broadcastowych (rozgłoszeniowych), spotykanych w szeroko stosowanych technologiach LAN z dzielonym medium np. w sieciach typu Ethernet. We wspomnianych technologiach multicasting umożliwia wielu systemom końcowym jednocześnie nadawanie i odbieranie danych od wielu innych systemów końcowych. Takie możliwości są proste do zaimplementowania w przypadku wspólnego (dzielonego) medium, gdy każda ze stacji ma dostęp do wszystkich transmisiowanych danych. Oczywistą analogią w systemach ATM mogłyby być zestawienie dwukierunkowego połączenia wielu-do-wielu (ang. *multipoint-to-multipoint connection*). Niestety, to proste rozwiązanie nie może zostać wprowadzone dla AAL5, czyli w przypadku najczęściej używanego do transmisji danych typu protokołu warstwy adaptacji. W przeciwieństwie do klasy AAL3/4, używającej identyfikatorów komunikatów MID (ang. *Message Identifier*), AAL5 nie posiada w formacie komórki żadnego pola pozwalającego na przeplatanie komórek z różnych pakietów AAL5 (gdzie pakiet jest rozumiany jako seria komórek przenoszących pojedynczą wiadomość z warstw wyższych (np. dane użytkownika)) transmitowanych w obrębie jednego połączenia. Oznacza to, że poszczególne pakiety AAL5 wysypane do danego odbiorcy przez dane połączenie muszą zostać odebrane w kolejności i nie mogą być przeplatane z innymi pakietami. W innym przypadku stacja odbierająca nie będzie w stanie odtworzyć otrzymanej informacji. Z tego powodu oferowane przez sieć ATM połączenia jeden-do-wielu muszą być jednokierunkowe.

Aby uporać się z powstającym problemem ATM Forum zaproponowało trzy alternatywne rozwiązania:

- **VP-Multicasting** - Mechanizm ten, do realizacji połączeń typu wielu-do-wielu, wykorzystuje ścieżkę wirtualną o ustalonym identyfikatorze VPI, w której każda ze stacji końcowych posiada unikatowy numer VCI. Przeplatane pakiety, pochodzące od różnych stacji końcowych, mogą być więc rozróżniane przy użyciu tych identyfikatorów VCI.
- **Multicast Server** - W tym przypadku każda stacja wchodząca w skład grupy wymieniającej dane w trybie wielu-do-wielu utrzymuje połączenie typu punkt-punkt ze specjalnym urządzeniem, określonym jako Multicast Server. Serwer taki retransmituje dane otrzymane od poszczególnych stacji do pozostałych dbając, aby pakiety danych nie przeplatały się wzajemnie. Wykorzystanie serwera typu „Multicast” ilustruje rysunek 7.21.



Rys. 7.21. Ilustracja działania serwera typu „Multicast”



Rys. 7.22. Ilustracja połączeń typu Overlaid Point-to-Multipoint

- *Overlaid Point-to-Multipoint Connections* - W tym przypadku każda stacja wchodząca w skład komunikującej się grupy utrzymuje jedno-kierunkowe połączenia typu jeden-do-wielu ze wszystkimi pozostałymi stacjami, zgodnie z ilustracją zawartą na rysunku 7.22.

Z zaprezentowanych rozwiązań, obecnie najczęściej spotykane w praktyce są dwa ostatnie, przy czym pierwsze z nich jest łatwiejsze w realizacji i wymaga mniej zasobów sieciowych.

## 7.6 Przyszłość ATM

W chwili obecnej ATM jest powszechnie akceptowane jako technika przyszłości. Żadna inna technologia sieciowa nie oferuje bowiem równie elastycznych rozwiązań. Z jej usług coraz częściej korzystają też użytkownicy sieci LAN, uzyskując za pośrednictwem sieci ATM dostęp do Internetu.

W najbliższym okresie sieci ATM będą w coraz szerszym zakresie pełnić funkcje szybko pracujących systemów szkieletowych, obsługujących standardowe aplikacje (opracowane głównie z myślą o pracy w środowiskach LAN).

Można wymienić co najmniej dwa sposoby wykorzystania sieci ATM do obsługi aplikacji. Pierwszym jest fragmentacja ramek LAN, czyli dzielenie na mniejsze części różnych ramek standardu 802.x i „zaginieżdżanie” ich (enkapsulacja) w komórkach sieci ATM. Drugi sposób sprowadza się do „zaginieżdżania” w strukturach ATM pakietów warstwy sieciowej.

Organizacja ATM Forum zdecydowała się na wspieranie pierwszego sposobu i opracowała stosowną specyfikację, znaną jako LAN Emulation, której szerszy opis podany zostanie w rozdziale 10. Istota pracy protokołu emulacji sieci LAN w sieci ATM polega na tym, że sieć ATM jest niewidoczna (logicznie) dla świata zewnętrznego, tak więc użytkownicy sieci LAN mogą łączyć się z sieciami ATM używając standardowych interfejsów, np. ODI (ang. *Open Data-Link Interface*) firmy Novell lub NDIS (ang. *Network Device Interface Specification*) firmy Microsoft. ATM Forum opublikowało specyfikację LANE (wersja 1.0) w styczniu 1995, wersja 2.0 LANE jest obecnie w końcowej fazie przygotowań.

Z kolei organizacja Internetu IETF (ang. *Internet Engineering Task Force*) wybrała inną drogę niż ATM Forum, proponując współpracę pomiędzy sieciami pakietowymi LAN/WAN, a siecią ATM, na poziomie warstwy sieciowej. IETF opublikowała początkowo dwie wstępne wersje tego standardu: RFC 1483 i RFC 1577. Jako standard zatwierdzona została druga z tych propozycji, znana pod nazwą „Classical IP and ARP over ATM”. W tym standardzie, adresy protokołu IP poddawane są konwersji na adresy sieciowe stacji końcowych sieci ATM. Adres IP jest używany do definiowania adresu podsieci, do której należy stacja końcowa ATM. Ten sposób konwersji adresów umożliwia kompleksową obsługę ruchu pakietów w sieciach LAN i ATM połączonych w jeden „organizm”. ATM Forum utworzyło

też dwie inne grupy robocze, które pracują nad modyfikacjami rozwiązań współpracy sieci pakietowych i ATM w warstwie sieciowej. Ponieważ jest to ta warstwa, w której odbywa się routing pakietów, nowe koncepcje opracowywane przez te grupy zmieniają prawdopodobnie rolę routerów w sieciach komputerowych. Pierwsza opcja jest oparta na standardzie MPOA (ang. *MultiProtocol Over ATM*), dopracowywanym obecnie przez projektantów. Zwolennikami tej opcji są firmy Cisco i Newbridge. MPOA zakłada, że używane obecnie przez sieci LAN protokoły będą poddawane konwersji (chodzi tu o adresy) na standard ATM przez specjalne serwery routingu. Serwer taki pełniłby funkcję szeroko rozumianego serwera katalogów, znającego adresy ATM tych stacji, które są zlokalizowane najbliżej danej sieci LAN. Drugie rozwiązanie, dotyczące również współpracy w trzeciej warstwie modelu OSI, nosi nazwę I-PNNI (ang. *Integrated Private-Network-Network Interface*). Jest to koncepcja popierana przez IBM, 3Com i Bay Networks. W standardzie I-PNNI sieć ATM używa swojego własnego protokołu routingu, który rozpoznaje topologię sieci i zawiaduje adresami, umożliwiając w ten sposób integrację tradycyjnych sieci LAN (i pracujących w nich stacji) z sieciami ATM. Jeszcze inne rozwiązanie proponuje firma Ipsilon Networks, która z kolei wyposaża każdy przełącznik ATM w inteligentne moduły oprogramowania, wyznaczające pakietom trasy ich przesyłu. Proste pakiety, w rodzaju poczty elektronicznej, są kierowane za każdym razem do routera. Natomiast te strumienie pakietów, które są przesyłane przez dłuższe okresy (np. grafika komputerowa przesyłana przez serwery sieci WWW), są od razu transmitowane przez wirtualne łącza zestawiane przez sieci ATM.

Być może czynnikiem przyspieszającym proces przechodzenia na technologię ATM będzie zestaw specyficznych usług typu QoS świadczonych przez te sieci. Kontrola jakości usług QoS oferowana przez sieci ATM przydaje się najbardziej wtedy, gdy łącze jest bardzo obciążone i realizacja aplikacji musi być niezawodna, a ekspedowane przez nią dane winny być przesyłane z odpowiednio dużą szybkością.

Dotychczasowe rozwiązania protokolarne stosowane w sieciach pakietowych (np. IPv4 w Internecie) nie pozwalały użytkownikom sieci LAN na pełne korzystanie z rozwiązań oferowanych przez sieci ATM. Bezpośredniowy przekaz, realizowany w większości sieci LAN, MAN i WAN, mógł być przenoszony, poprzez sieci ATM, za pośrednictwem protokołów AAL 3/4 ATM, a jedną dostępną usługą warstwy ATM mogła być usługa UBR. Oczekuje się, że nowy protokół Internetu, IPv6, definiujący szereg klas priorytetów ruchu wpłynie na zmianę tej sytuacji.

Z sieciami ATM przemawia też fakt, że standard QoS jest wspierany przez coraz więcej firm. Systemy operacyjne Windows NT i Windows 95 będą już niedługo dysponować łączami programistycznymi WinSock 2 API, dzięki którym aplikacje będą mogły korzystać z usług sieci ATM, definiując konkretne żądanie co do przepustowości łącza. Innym aspektem przemawiającym za stosowaniem techniki ATM w sieciach LAN są różnorodne aplikacje multimedialne, w tym aplikacje

graficzne (CAD/CAM), duże bazy danych integrujące dane i grafikę (GIS) oraz wiele innych nowoczesnych zastosowań wymagających coraz większych szybkości przesyłania danych między komputerami, a szczególnie między serwerami a innymi użytkownikami sieci. Jedno jest pewne, technika ATM będzie stosowana w sieciach rozległych. Natomiast jeśli chodzi o sieci lokalne, to można się spodziewać, że dojdzie tu do ostrej konfrontacji między ATM i innymi konkurencyjnymi technologiami (np. Fast Ethernet, Giga Ethernet czy 100VG-AnyLAN). Wszystko wskazuje na to, że przyjęcie konkretnych rozwiązań (jeśli chodzi o architekturę łączą ATM sprzągających sieci komputerowe) zależy będzie w większej mierze od pozycji producenta na rynku niż aktualnego stanu standardów.

## 8 Wersja 6 protokołu IP

Zestaw protokołów TCP/IP został opracowany w połowie lat siedemdziesiątych na potrzeby sieci ARPA. Nieoczekiwany sukces komercyjny i użytkowy sprawił, że na początku lat osiemdziesiątych protokoły te uznano powszechnie za nieoficjalny standard sieciowy. *Spontaniczny rozwój ogólnoświatowej sieci Internet, będącej sukcesorką sieci ARPA, utrwałało znaczenie pary protokołów TCP/IP: internetowego protokołu międzymiędzysieciowego IP i transportowego protokołu TCP, jako protokołów najpopularniejszych i najszerzej stosowanych (por. rozdział 1.3.4) w funkcjonujących sieciach komputerowych.* Do istotnych zalet tych protokołów można przy tym zaliczyć:

- możliwość integracji różnych systemów sieciowych,
- otwartość i niezależność od specyfiki sprzętowo-programowej łączonych sieci,
- jednoznaczność systemu adresacji użytkowników,
- wspomaganie różnorodnych usług aplikacyjnych.

### 8.1 Internetowy protokół IP

Najważniejszym protokołem warstwy sieciowej w architekturze TCP/IP jest protokół internetowy IP (ang. *Internet Protocol*). Został on zdefiniowany w dokumencie RFC 791. IP jest typowym protokołem bezpołączniowym, służącym do przekazu datagramów. Z tego powodu jest on często określany mianem protokołu zawodnego (niewiarygodnego).

Podstawowymi jednostkami danych, definiowanymi przez protokół IP, są datagramy. Datagramy przesypane są przez sieć niezależnie od siebie. Oznacza to możliwość ich transmisji różnymi trasami, nawet jeśli zawierają fragmenty wiadomości przeznaczonej do tego samego adresata. Protokół IP ściśle określa format datagramu przesyłanego w sieci Internet. Miejsce przeznaczenia datagramu IP rozpoznawane jest na podstawie adresu odbiorcy, umieszczonego w nagłówku każdego datagramu IP. Różne wersje protokołu IP definiują różne formaty nagłówków datagramów. Należy dodać, że IP odpowiada zarówno za tworzenie datagramów jak i, w razie konieczności, ich fragmentację (podział) i ponowne odtwarzanie.

Protokół IP ma szereg wersji. Powszechnie stosowaną jest obecnie wersja 4 (opisana w rozdziale 1.3.4). Przewiduje się, że w niedalekiej przyszłości do użytku wprowadzona zostanie wersja 6 (IPv6), stanowiąca element nowej generacji protokołów IP. Ogólną koncepcję i podstawowe funkcje tych protokołów zdefini-

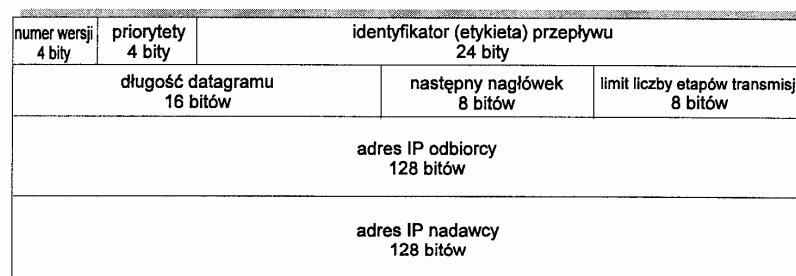
wano w dokumencie RFC 1726 (*Technical Criteria for Choosing the Next Generation - IPng*). W dwóch kolejnych paragrafach niniejszego rozdziału zaprezentujemy podstawowe cechy protokołu IPv6 i przykładowe zmiany w porównaniu z wersją 4.

## 8.2 Podstawowe cechy protokołu IPv6

*Kolejna, 6 wersja protokołu IP wprowadza, w porównaniu z wersją 4, szereg istotnych modyfikacji. Zmianie ulega między innymi postać i znaczenie niektórych pól nagłówka datagramu.* W szczególności w IPv6 mamy:

- nowy, 128-bitowy system adresowania,
- udoskonaloną postać nagłówka IP, z rozszerzeniami dla aplikacji i opcji,
- nowe pole kontrolne zwane etykietą przepływu (ang. *flow control label*),
- brak sumy kontrolnej,
- zabezpieczenie przed zjawiskiem tzw. fragmentacji pośredniej (ang. *intermediate fragmentation*),
- wbudowane narzędzia kryptograficzne i mechanizmy uwierzytelniania adresata i nadawcy.

Nagłówek IP różni się więc istotnie od zaprezentowanego wcześniej nagłówka wersji 4 IP. Przede wszystkim posiada on nowe 128 bitowe adresy nadawcy i odbiorcy. Nie zawiera natomiast kilku innych pól, które w praktyce okazały się mało przydatne. Nowy format nagłówka IPv6 ilustruje rysunek 8.1.



Rys. 8.1. Nagłówek datagramu IPv6

Nagłówek datagramu IPv6 rozpoznawany jest poprzez umieszczenie w 4 bitowym polu numeru wersji liczby 6. Kolejne 4 bitowe pole określa priorytet datagramu. Nadawanie datagramom różnych priorytetów ma większe znaczenie niż w poprzedniej wersji. Jednym z kryteriów klasyfikacji datagramów jest ich wrażliwość na przeciążenie sieci. Datagramy mniej wrażliwe na przeciążenie, a jednocześnie mniej ważne z punktu widzenia konieczności ich „doręczenia”, mają w sieci niższy priorytet. W przypadku wystąpienia stanu przeciążenia ich przekaz jest czasowo

wstrzymywany, do momentu rozładowania przeciążenia w sieci. Pierwszy bit pola priorytetu określa bądź małą wrażliwość datagramów na przeciążenie (0), bądź też ich dużą wrażliwość (1). Priorytety nadawane datagramom i ich znaczenie ilustruje tabela 8.1.

Tabela 8.1. Wartości priorytetów datagramów i odpowiadające im rodzaje ruchu

wartość priorytetu	znaczenie datagramu
0	brak priorytetu
1	ruch „w tle”
2	transfer danych bez nadzoru
3	nie zdefiniowane
4	nadzorowany przepływ danych
5	nie zdefiniowane
6	interaktywny przepływ danych
7	informacje sterujące i zarządzające

Najwyższy (zdefiniowany dotychczas) priorytet posiada informacje sterujące przepływem w sieci i zarządzające pracę sieci. Przykładem datagramów z priorytetem 6 są dane przesypane w ramach aplikacji TELNET. Do kategorii 4 zaliczamy przekaz plików FTP. Przykładem kategorii 2 może być poczta elektroniczna, a kategorii 1 - newsy lub inne materiały o znikomej pilności. Datagramy, którym przypisano numery od 8 do 15, należą do grupy niewrażliwych na przeciążenie sieci. Ich klasyfikacja priorytetowa nie została jeszcze ustalona. Przewiduje się możliwość ich użycia do współpracy z siecią ATM i wykorzystanie przy realizacji usług o zadanej jakości QoS.

Całkowitą nowością nagłówka IPv6 jest pole identyfikatora (etykiety) przepływu (ang. *flow label*). Wartość tego pola jest identyczna dla wszystkich datagramów będących częścią tej samej wiadomości przesyłanej między dwoma ustalonymi urządzeniami końcowymi. Zgodnie z koncepcją IPv6 wszystkie datagramy wiadomości, opatrzone tą samą etykietą, będą przesyłane tą samą trasą. Oczekuje się, że spowoduje to znaczne przyśpieszenie transmisji. Brak nowego datagramu o tej samej etykiecie, przez okres co najmniej 6 sekund, będzie oznaczał zakończenie transmisji danej wiadomości. Pole etykiety przepływu, jest szczególnie ważne dla aplikacji uwarunkowanych czasowo, takich jak przekaz mowy i obrazów (np. wideokonferencje). Aplikacje, które nie chcą wykorzystywać etykiety przepływu, ustalają jej wartość na zero.

16 bitowe pole długości datagramu IPv6, odmiennie niż w wersji 4, określa długość danych nie uwzględniając przy tym długości nagłówka. Długość tego pola umożliwia tworzenie datagramów nie przekraczających 65535 bajtów. Dodatkowe opcje

IPv6 (opisane dalej) pozwalają jednakże na przesyłanie dłuższych datagramów. Zerowa wartość pola długości wskazuje na to, że rzeczywista wielkość datagramu podana będzie w polu dodatkowego nagłówka tzw. opcji międzywęzłowych (ang. *hop-by-hop*).

Kolejne 8-bitowe pole, nazywane polem następnego nagłówka (ang. *next header*) sygnalizuje wystąpienie w datagramie IP dodatkowego nagłówka z jego własnymi opcjami.

Następne, również 8-bitowe pole, określa maksymalną liczbę węzłów na trasie datagramu. Po każdorazowym przejściu datagramu przez węzeł wartość tego pola jest zmniejszana o 1, a osiągnięcie wartości zerowej powoduje usunięcie datagramu. Rozwiążanie proponowane w IPv6 dopuszcza stosowanie szeregu kolejno po sobie występujących nagłówków z właściwymi im rozszerzeniami. Datagram IP rozrasta się więc, w stosunku do wersji 4, wyraźnie umożliwiając przesyłanie wielu informacji użytecznych dla aplikacji. Kolejność występowania po sobie poszczególnych nagłówków jest ściśle zdefiniowana. Wybrane znaczenia dodatkowych nagłówków przedstawia tabela 8.2.

Tabela 8.2. Znaczenie i kolejność występowania opcjonalnych nagłówków rozszerzeń

Wartość występująca w polu „następny nagłówek”	Rola i znaczenie dodatkowego nagłówka
0	Nagłówek opcji międzywęzłowych ( <i>hop-by-hop</i> )
43	Nagłówek routingu
44	Nagłówek segmentacji
50	Nagłówek bezpieczeństwa enkapsulacji (szycfrowania danych)
51	Nagłówek uwierzytelniania
60	Nagłówek opcji adresata (aktualizowany tylko w miejscach przeznaczenia)

Nagłówki te pozwalają na realizację szeregu ważnych funkcji poprawiających efektywność i elastyczność pracy sieci Internet. I tak:

- Nagłówek opcji międzywęzłowych umożliwia między innymi zdefiniowanie długości datagramu przekraczającej 65535 bajtów. Pole nagłówka tzw. opcji Jumbo Payload pozwala na tworzenie datagramów o długości do 4 GB;
- Nagłówek routingu pozwala stacji źródłowej zdefiniować jeden lub więcej węzłów pośrednich na trasie przesyłu datagramu;
- Nagłówek segmentacji informuje o podziale datagramu na mniejsze fragmenty. IPv6 zakłada, iż dokonywanie podziału datagramu jest możliwe wyłącznie przez stację źródłową;
- Nagłówek opcji adresata (opcji przeznaczenia) pozwala na analizę datagramów wrażliwych na opóźnienia wyłącznie w węźle docelowym. Dopusz-

ca się również opcję, zgodnie z którą analiza datagramu dokonywana jest zarówno w węźle będącym tzw. pierwszym miejscem przeznaczenia, którego adres zawarty jest w polu adresowym nagłówka datagramu IPv6, jak też w węzłach kolejnych określonych w nagłówku routingu;

- Nagłówki uwierzytelniania uprawnienia i szycfrowania danych pozwalają podnieść bezpieczeństwo dostępu do sieci oraz transmisji danych.

We współczesnych sieciach komputerowych coraz większą wagę przywiązuje się do problemów bezpieczeństwa danych przechowywanych i przesyłanych w sieci. Zagadnienia te znajdują swoje odzwierciedlenie w mechanizmach wbudowanych w protokoły IPv6 (zabezpieczenia te występują również w rozszerzonej wersji IPv4). Są one zagwarantowane poprzez opcję uwierzytelniania i szycfrowania danych. Opcja ta zapewnia:

- integralność przesyłanych danych,
- uwierzytelnianie zarówno nadawcy jak i odbiorcy,
- jednoznaczne ustalanie nadawcy datagramu,
- tajność przesyłanych datagramów.

Trzy pierwsze cechy gwarantują zastosowanie dodatkowego nagłówka uwierzytelniającego AH (ang. *Authentication Header*). Z kolei tajność zapewnia mechanizm ESP (ang. *Encapsulated Security Payload*) szycfrowania całego datagramu, bądź przenoszonych przez niego danych, z wykorzystaniem algorytmu DES-CBC, będącego wzmacnionym algorytmem DES (ang. *Data Encryption Standard*). W zależności od „zasięgu” szycfrowania mamy dwie wersje ESP określone jako:

- tunelowanie, gdy cały datagram IP jest szycfrowany i przesyłany jako dane zwykłego pakietu IP, bądź
- transport-mode ESP, gdy dane przenoszone przez datagram IP są kodowane i poprzedzane nagłówkiem ESP.

Nowe standardy IP dopuszczają oczywiście łączenie metod AH i ESP, dla pełniejszego zabezpieczenia przesyłanych informacji. O ile implementowanie funkcji AH/ESP jest opcjonalne dla rozszerzonej wersji IPv4, o tyle dla protokołu IPv6 jest ono wymagane.

W wersji 6 protokołu IP został wprowadzony schemat weryfikacji zwany MD5 (ang. *Message Digest 5*). Schemat ten opiera się na tak zwanym indeksie parametrów zabezpieczenia, po którym następują 16 bajtowe dane weryfikacyjne. W oparciu o te dane wyliczane jest 128 bitowe słowo kodowe, zarówno w stacji nadawczej jak i odbiorczej. Otrzymanie identycznej wartości kodowej oznacza poprawność przesyłanych danych.

### 8.3 Adresacja w protokole IPv6

Dwa ostatnie pola nagłówka IPv6g zawierają 128-bitowe adresy nadawcy i odbiorcy. Umożliwiają one stworzenie ogromnej liczby adresów, które tym samym przez

dłuższy czas powinny być wystarczające do obsługi ciągle rosnącej liczby użytkowników sieci Internet. Nowa struktura adresowania pozwala wyróżnić:

- adresy proste, identyfikujące pojedyncze interfejsy odbiorcze (tzw. adresy typu unicast),
- adresy grupowe, identyfikujące grupy interfejsów należących zwykle do różnych urządzeń sieciowych (tzw. adresy typu multicast),
- adresy identyfikujące wybrane interfejsy danej grupy (tzw. adresy typu anycast).

Definiowanie pola adresowego nie zostało jeszcze zakończone. Wiadomo jednak, że obejmuje ono zarówno dotychczasowe adresy 32-bitowe, jak też adresy:

- NSAP, gwarantujące kompatybilność z adresacją ISO,
- IPX, uwzględniające potrzeby systemu sieciowego Novell NetWare,
- zarządzane przez operatorów,
- lokalne,
- grupowe.

*Ważną cechą nowego systemu adresacji jest pełna obsługa dotychczasowych adresów 32-bitowych. Adresy IPv6, wszystkich typów, są przypisywane interfejsom węzłów (stacji roboczych, komputerów obliczeniowych, routerów) a nie samym węzłom. Ponieważ jednak każdy interfejs należy do jednego urządzenia, do wolny z adresów unicastowych węzła może być użyty jako jego identyfikator.*

Grupa robocza IETF opracowała trzy formy prezentacji adresów IPv6, w postaci ciągów znaków tekstowych:

Forma 1:

Preferowaną postacią adresu IPv6 jest:

x:x:x:x:x:x:x:x, gdzie "x" jest wartością heksadecymalną reprezentującą 16 bitową część adresu.

Forma 2:

Zgodnie z założoną przez projektantów, znaczną nadmiarowością adresów IPv6, w adresie mogą się pojawiać długie ciągi zer. W celu uproszczenia zapisu takich adresów wprowadza się specjalną metodę składniową, pozwalającą na "kompresję" zer w prezentowanym adresie. Kompresja zaznaczona jest podwójnym dwukropkiem. Użycie symbolu ":" wskazuje więc na obecność, w adresie rzeczywistym, jednej lub wielu grup 16-stu kolejnych zer. Przykładowo, adres multicastowy o postaci: FF01:0:0:0:0:48 może być zapisany jako FF01::48. Symbole ":" mogą się przy tym pojawiać w „skróconym” adresie tylko raz (FF01 jest w powyższym przykładzie przedrostkiem wskazującym na multicastowy typ adresu).

Forma 3:

Alternatywną postacią adresu, zalecaną do użycia w przypadku środowisk węzłów sieci IP stosujących adresy IPv4 i nowe adresy IPv6, jest:

x:x:x:x:x:x:d.d.d

W powyższym zapisie 6 kolejnych symboli "x" reprezentują 96 symboli binarnych adresu IPv6, poprzedzających 32 bity adresu IPv4. Zgodnie z podaną wcześniej konwencją, "x" oznacza wartość heksadecymalną każdego z sześciu bardziej znaczących 16-sto bitowych fragmentów adresu. Z kolei symbole "d" są wartościami dziesiętnymi czterech mniej znaczących 8-mio bitowych części adresu. Przykładowe postacie tego typu adresów, to:

0:0:0:0:0:17.1.78.5 lub

0:0:0:0:FFFF:139.154.53.38

W formie skróconej (tj. po kompresji) adresy te przyjmują postać

::17.1.78.5

::FFFF:139.154.53.38

Projektanci nowego schematu adresacji IPv6 przewidują możliwość koegzystencji i współpracy obu systemów tj. IPv6 i IPv4. W przypadku przesyłania pakietów IPv6 poprzez infrastrukturę routingową IPv4, opracowane zostały techniki dynamicznego tunelowania datagramów IPv6. Opracowano też specjalne unicastowe adresy IPv6 pozwalające na przenoszenie adresów IPv4, za pośrednictwem 32 mniej znaczących bitów adresu 128-bitowego. Pierwszy typ adresu, określany mianem "IPv4 kompatybilny z IPv6" (ang. *IPv4 - compatible IPv6 address*) ma w zapisie nieformalnym postać:

0:0:0:0:0:adres IPv4.

96 początkowych zer stanowi tutaj przedrostek charakteryzujący rodzaj adresu (w tym przypadku przenoszenie adresu IPv4 w postaci kompatybilnej z IPv6).

Opracowano też drugą, podobną w swej postaci, wersję adresów IPv6 przenoszących umieszczone w ich strukturze adresy IPv4. Wersja ta nazywana "IP – mapped IPv6 address" ma w zapisie nieformalnym postać:

0:0:0:0:FFFF:adres IPv4.

Jest ona przewidziana do obsługi węzłów nie wspomagających nowego systemu adresacji IPv6.

Obie opisane powyżej metody adresacji IPv6 z "włożonymi" adresami IPv4 wykorzystują trzecią formę prezentacji adresu.

*Cechą charakterystyczną nowej 128-bitowej wersji adresów IP jest to, że składają się one z bitów przedrostka i adresu właściwego. Ta ciekawa metoda prefiksu i numeru właściwego uelastycznia system adresacji.* Dla przykładu: przedrostek 010 (ewentualnie 100) oznacza globalny adres typu unicast (pojedynczego urządzenia lub interfejsu programowego).

0000001 - adres NSAP,

0000010 - adres IPX,

111111101 lub 1111111011 - adres „unicastowy” wykorzystywany lokalnie,

11111111 - adres multicastowy (FF).

Propozowany, dodatkowo, nowy podział na strefy geograficzne powinien zagwarantować sprawniejsze funkcjonowanie algorytmów routingu.

W chwili obecnej rozdzielone zostało około 15 % przestrzeni adresowej. Pozostałe 85 % zarezerwowano do przyszłego użytku.

Nowe, wspomniane powyżej kategorie adresów: unicast, multicast i anycast oferują też inne ciekawe możliwości.

Adresy proste, czyli typu „unicast” pozwalają identyfikować jeden określony interfejs odbiorczy. Umożliwiają tym samym adresację datagramów, kierowanych np. do określonej stacji PC i do właściwego protokołu, bez obawy, że datagramy te zostaną przejęte przez inne oprogramowanie stacji.

Z kolei adresy grupowe („multicast”) identyfikują zestawy interfejsów należących zwykle do różnych węzłów. Przejęły one rolę adresów broadcastowych (i multicastowych) z IPv4. Datagram tego typu dotrze do wszystkich interfejsów danej grupy, tj. identyfikowanych określonym adresem typu multicast. Opcja ta jest jednakże efektywniejsza od rozwiązania typu broadcast z IPv4 (gdzie rozgłaszczenie typu multicast wymagało stosowania niejasnego adresowania klasy D), gdyż zakres pojedynczego adresu grupowego może być ustalany elastycznie (z ograniczeniem do systemu, określonego miejsca, powiązanego z łączem bądź też globalny).

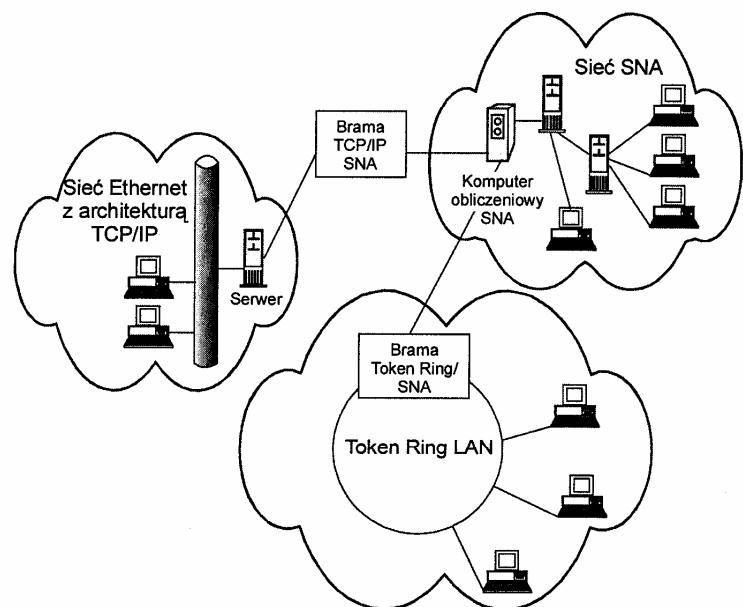
Adresy typu „anycast” pozwalają na identyfikację zestawu interfejsów należących zwykle do różnych węzłów. Umożliwia to przesyłanie datagramu do jednego, zwykle najbliższego, spośród interfejsów identyfikowanych tym zmodyfikowanym adresem grupowym (np. najbliższego routera).

## 9 Łączenie sieci - przegląd metod i układów pośredniczących

*Przy łączeniu sieci komputerowych, bądź też przy przyłączaniu do nich różnych urządzeń końcowych, należy rozwiązać szereg problemów wynikających z niedopasowania fizycznego lub logicznego łączonego sprzętu.* Typowe sytuacje i wymagania związane z łączeniem sieci lub przyłączaniem do nich nowych stacji można zilustrować kilkoma charakterystycznymi przykładami.

- W przypadku łączenia komputerów osobistych, bądź ich dołączania do sieci, musimy spełnić stosowne wymagania w zakresie zarówno okablowania i sprzęgu (interfejsu) sieciowego jak i wyposażenia stacji we właściwe adaptery sieciowe. Wzajemna współpraca stacji w sieci LAN wiąże się więc przede wszystkim z zapewnieniem zgodności z wymaganiami specyfikowanymi przez standardy w zakresie warstwy fizycznej i warstwy łącza danych (modelu ISO-OSI). Przyłączanie nowych stacji może się przy tym odbywać zarówno za pośrednictwem specjalizowanych układów sprzągających, jak też poprzez serwery sieciowe, z wykorzystaniem portów do asynchronicznej transmisji szeregowej.
- Łączenie czy też rozbudowa sieci LAN, zarówno tych o jednakowych standardach MAC (i LLC), poza wymiary narzucone wymaganiami technicznymi, jak też sieci LAN o odmiennych standardach, wymaga rozwiązania szeregu specyficznych zagadnień, dotyczących głównie funkcji realizowanych przez warstwę fizyczną i łącza danych. Problemy, z którymi się wówczas stykamy, wiążą się z różnymi rodzajami wykorzystywanych mediów, różnymi szybkościami pracy, z odmiennością formatów ramek i występowaniem, bądź nie, specyficznych pól ramek. Często, w przypadku łączenia sieci LAN lub MAN, nawet o identycznych architekturach logicznych, w struktury o rozbudowanej, złożonej topologii, z dużą liczbą różnorodnych urządzeń końcowych, względы niezawodnościowe bądź wymagania odnośnie elastycznego i efektywnego sterowania przepływem informacji narzucają konieczność rozwiązywania problemów routingu i zagadnień adresowania na poziomie warstwy sieciowej.
- Nieco odmienna sytuacja ma miejsce, gdy poszczególne sieci (LAN, MAN, WAN), czy też komputery o zaimplementowanych różnych architekturach logicznych, np. OSI, SNA, TCP/IP, wykorzystują wspólną podsieć komunikacyjną do przekazu informacji między rozproszonymi lecz jednorodnymi logicznie zespołami tych sieci. Sytuację taką ilustruje rysunek 9.1. Mamy wówczas do czynienia z tzw. sieciami wirtualnymi.

Problemy wymagające rozstrzygnięcia związane są wówczas z funkcjonowaniem warstw drugiej i trzeciej, tj. łącza danych i warstwy sieciowej. Dotyczą one formatów pakietów, zasad adresacji w sieciach, zasad routingu (wyboru tras) i sterowania przepływem na poziomie warstwy łącza danych i sieciowej.



Rys. 9.1. Ilustracja łączenia sieci o różnych architekturach logicznych

- Najwięcej problemów technicznych pojawia się w przypadku łączenia i wzajemnej współpracy sieci o odmiennych architekturach logicznych. Chęć zapewnienia współpracy pomiędzy aplikacjami tych sieci musi po ciągać za sobą dokonywanie konwersji i/lub emulacji protokołów wszystkich warstw; w szczególności zrozumiane i jednoznacznie interpretowane muszą być komendy i odpowiedzi związane z realizacją aplikacji.

## 9.1 Przykłady wzajemnego niedopasowania rozwiązań sieciowych w wybranych standardach sieci LAN i MAN

*Niekompatybilność rozwiązań sieciowych manifestuje się w różnych formatach ramek i różnej ich maksymalnej długości, występowaniu, bądź też nie, priorytetów czy też różnej kolejności przesyłania bitów. Odmienne parametry*

**popularnych standardów sieciowych i istotne różnice w ich funkcjonowaniu rodzą określone problemy przy wzajemnej współpracy tych standardów.** Poniżej prezentujemy wpływ wybranych parametrów sieci na złożoność algorytmów współpracy.

### Format ramki

Każdy z opisanych w książce standardów sieci komputerowych używa innego formatu ramki (por. rozdz. 4). Różnice w formatach ramek dla poszczególnych standardów powodują konieczność zmiany tych formatów podczas przesyłania ramek pomiędzy różnymi typami sieci. Operacja taka jest zwykle czasochłonna oraz zasobochłonna, wymaga bowiem użycia procesora i pamięci. Zmiana formatu ramki wiąże się między innymi z obliczeniem nowej sumy kontrolnej. Może to prowadzić do powstania niewykrywalnych błędów, np. na skutek przekłamań w pamięci urządzenia przegązającego sieci.

### Maksymalna długość ramki

Pośczezugłe standardy przewidują odmienne maksymalne długości ramek (patrz tabela 9.1). Jeżeli rama jest zbyt dłuża, by przesłać ją do sąsiedniej sieci, musi ona ulec odrzuceniu. Wynika to z faktu, że ani warstwa fizyczna ani też warstwa łącza danych, których dotyczą omawiane standardy, nie mogą dzielić ramek na mniejsze fragmenty, a następnie ich składać. Innym, możliwym rozwiązaniem tego problemu jest wykorzystanie do fragmentacji przesyłanych jednostek danych protokołów warstw wyższych (por. np. protokół IP), które umożliwiają segmentację i składanie ramek.

Tabela 9.1. Maksymalne długości ramek, szybkości transmisji i priorytety ramek dla wybranych standardów sieci LAN i MAN

Standard	Maksymalna długość ramki [w bajtach]	Szybkość transmisji [w Mb/s]	Priorytety
IEEE 802.3	1518/1526	1 do 20	brak
IEEE 802.4	8191	1, 5, 10, 20	4 poziomy
IEEE 802.5	4500 (dla szybkości 4Mb/s) <sup>1</sup> 8000 (dla szybkości 16 Mb/s) <sup>1</sup>	(1), 4, 16	8 poziomów (opcjonalnie)
ANSI X3T9.5 (FDDI)	4500	100	8 poziomów (dla ruchu asynchronicznego)
IEEE 802.6 (DQDB)	9188 (dla usługi bezpołączeniowej)	1.544 do 155	3 poziomy (opcjonalnie)

<sup>1</sup>) Standard 802.5 nie wprowadza górnego limitu, z wyjątkiem faktu, że stacja nie może transmitować dłużej, niż wynosi czas przetrzymywania tokenu.

W sieciach LAN, z uwagi na dużą szybkość transmisji, dużą odporność na zakłócenia i 4-bajtowe zabezpieczenie kodowe (ciąg kontrolny kodu cyklicznego), preferowane są długie bloki danych o długościach do 1500 bajtów (Ethernet) lub nawet znacznie większych (Token Bus, Token Ring, FDDI). Pozwala to na uzyskanie wysokiej efektywności transmisji.

W pakietowych, publicznych sieciach rozległych, z powodu stosunkowo niskiej jakości łączy i najczęściej jedynie 2-bajtowego zabezpieczenia kodowego, do transmisji dopuszczane są bloki znacznie krótsze. W sieciach X.25 stosowane są zwykle bloki o długościach 128 lub 256 bajtów (znacznie rzadziej stosowane są bloki o długościach 1024, 2048 czy też 4096 bajtów).

### Szybkość transmisji

Różne szybkości transmisji w poszczególnych, łączonych sieciach (patrz tabela 9.1) powodują, że przesyłanie dużej ilości informacji z sieci szybszej do wolniejszej, zwłaszcza jeżeli ta ostatnia jest silnie obciążona, może okazać się kłopotliwe. Konieczne jest wówczas buforowanie ramek w urządzeniu sprzągającym sieci. W przypadku zbyt dużej liczby ramek przesyłanych pomiędzy sieciami może nastąpić przepełnienie bufora, w wyniku którego część informacji zostanie stracona.

### Priorytety ramek

Niektóre standardy umożliwiają stosowanie kilku poziomów priorytetów (patrz tabela 9.1). Podczas przesyłania ramek z sieci stosującego priorytety do sieci, w której priorytety nie są używane, może mieć miejsce usuwanie priorytetów, które nie ma jednakże wpływu na jakość dalszej transmisji. W sytuacji odwrotnej ramkom muszą być nadawane fikcyjne priorytety, które mogą nie odzwierciedlać właściwego znaczenia przesyłanych ramek.

Przesyłanie ramek pomiędzy sieciami stosującymi różną liczbę poziomów priorytetów może być także kłopotliwe, gdyż następuje wtedy przekopiowanie priorytetu niezależnie od tego, czy jego wartość jest prawidłowo rozumiana przez sieć docelową, czy też nie.

### Kolejność przesyłanych bitów

W standardach dla sieci LAN i MAN brakuje jednolitych zasad dotyczących serializacji i deserializacji przesyłanych ciągów. W normach IEEE 802.3 i 802.4 przewiduje się, że jako pierwszy bit przesyłany jest najbardziej znaczący bit danego bajtu, z kolei w normach IEEE 802.5 i ANSI X3T9.5 bitem pierwszym jest bit najmniej znaczący. Urządzenia sprzągające muszą zatem, w odpowiednich przypadkach, odwracać porządek transmitowanych bitów.

### Sposób zapewniania poprawności transmisji

Innym źródłem niekompatybilności w rozwiązaniach sieciowych może być także przyjęcie różnych rozwiązań w zakresie zapewnienia jakości i bezpieczeństwa transmisji. Dla przykładu:

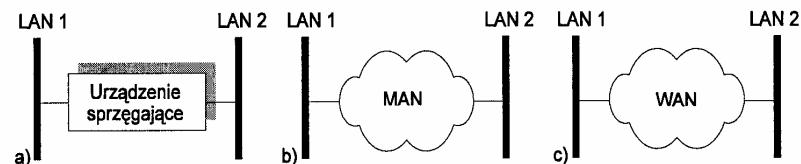
- w sieciach LAN stosowane jest zazwyczaj 4-bajtowe pole kontrolne kodu CRC-32; z kolei
- w sieciach WAN praktyczne zastosowanie znajdują kody cykliczne generowane przez wielomian CRC-16.

Urządzenia sprzągające muszą zatem dokonywać podwójnych przeliczeń sum kontrolnych.

## 9.2 Sposoby łączenia sieci LAN

Wzajemną komunikację pomiędzy sieciami LAN możemy zapewnić na kilka sposobów, w zależności od potrzeb, możliwości i odległości między sieciami. Wśród podstawowych wariantów wyróżnić można łączenie sieci (patrz rysunek 9.2):

- a) bezpośrednie, poprzez urządzenie sprzągające,
- b) za pośrednictwem sieci MAN oraz
- c) za pośrednictwem sieci WAN.



Rys. 9.2. Połączenie sieci LAN za pośrednictwem: a) urządzenia sprzągającego, b) sieci MAN, c) sieci WAN

Każdy z wymienionych wariantów wykorzystuje specjalizowane urządzenia, umożliwiające sprząganie sieci komputerowych. Urządzenia te pełnią więc kluczową rolę w procesie łączenia sieci LAN, MAN i WAN.

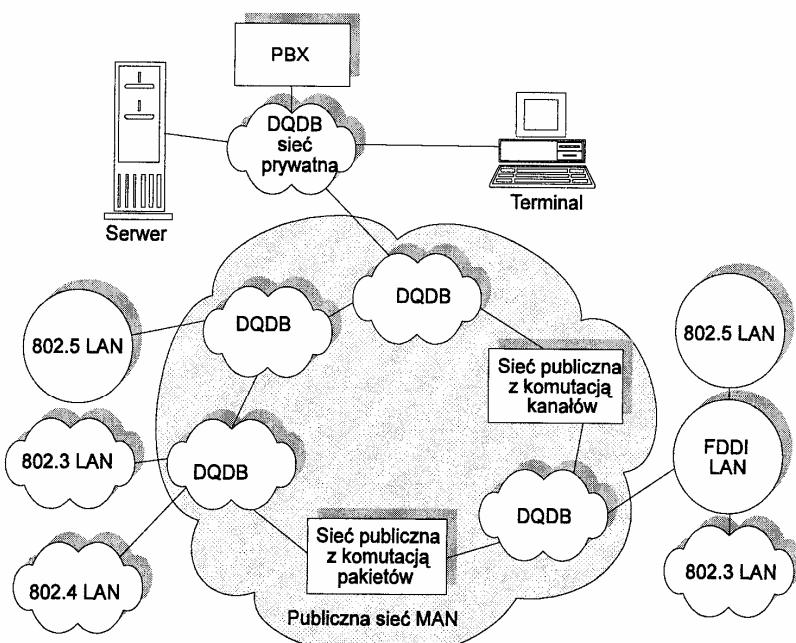
### Połączenie poprzez urządzenie sprzągające

Do łączenia bądź rozbudowy sieci LAN wykorzystuje się najczęściej urządzenia sprzągające (ang. *internetworking units*). Pod pojęciem tych urządzeń rozumiemy różne klasy sprzętu, od regeneratorów, poprzez huby, przełączniki, mosty, routery aż do konwerterów protokołów.

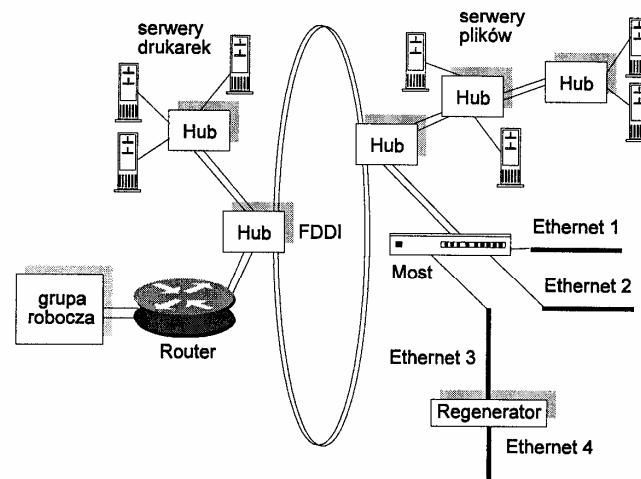
### Połączenie za pośrednictwem sieci MAN

W przypadku łączenia oddalonych od siebie sieci LAN konieczne jest, oprócz odpowiednich urządzeń sprzągających, wykorzystanie innej sieci, pośredniczącej w wymianie informacji pomiędzy sieciami lokalnymi. Jeżeli łączone sieci LAN znajdują się w odległości nie większej niż 50 km, to siecią pośredniczącą może

być sieć MAN. Podstawowymi standardami sieci MAN są przy tym sieci DQDB i FDDI. Przykładową sieć MAN, łączącą ze sobą różne typy sieci i urządzeń, pokazuje rysunek 9.3. W tym przypadku sieć zbudowana jest z kilku podsieci DQDB i stanowi przykład struktury publicznej sieci miejskiej. Połączenia pomiędzy podsieciami DQDB mogą być realizowane poprzez mosty lub routery, łącza "punkt-punkt" oraz sieci z komutacją pakietów lub z komutacją kanałów. Warto zauważać, że sieć FDDI pełni tutaj rolę sieci lokalnej. Technologia FDDI jest bowiem używana nie tylko do budowy sieci MAN, ale także do konstrukcji szybkich sieci lokalnych (ang. HSLN - *High Speed Local Networks*). FDDI może więc pełnić rolę sieci szkieletowych (ang. *backbone*) dla np. rozbudowanych sieci biurowych (ilustruje to rysunek 9.4). Sieć szkieletowa umożliwia obsługę znacznego ruchu pomiędzy stacjami i serwerami, jak też gwarantuje łatwe podłączenie do sieci nowej grupy roboczej, obejmującej np. inny wydział/oddział firmy. W przypadku, gdy dołączona grupa robocza potrzebuje bezpośredniego połączenia z FDDI, ale bez nadmiernego "rozgłaszenia" ramek (ang. *broadcast storms*), wówczas korzystnie jest dołączyć ją do sieci FDDI poprzez router. W celu obsługi większej liczby użytkowników możemy zwiększyć liczbę dedykowanych serwerów plików i drukarek.



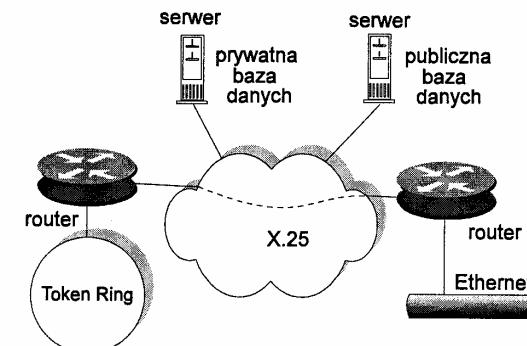
Rys. 9.3. DQDB - publiczna sieć MAN



Rys. 9.4. Sieć biurowa z arterią osiową FDDI

#### Połączenie za pośrednictwem sieci WAN

W przypadku, gdy odległość pomiędzy sieciami lokalnymi jest duża (większa niż 50 km) wykorzystuje się połączenia „komutowane” typu "punkt-punkt" realizowane poprzez sieć WAN. Przykład takiego wariantu łączenia sieci pokazano na rysunku 9.5. Dwie sieci lokalne (Ethernet i IBM Token Ring) zostały połączone ze sobą poprzez sieć rozległą z komutacją pakietów (X.25). Dołączenie sieci LAN do sieci WAN umożliwia im korzystanie zarówno z prywatnych, jak też z publicznych baz danych.



Rys. 9.5. Połączenie sieci LAN i baz danych poprzez sieć rozległą X.25

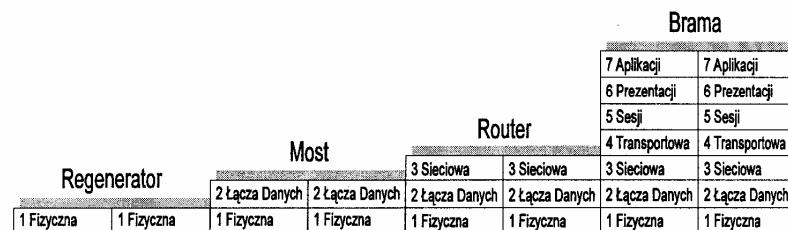
W omawianym przypadku należy rozstrzygnąć problemy związane z odmiennymi rozmiarami ramek w sieciach LAN i WAN (większy rozmiar ramek w sieciach lokalnych) oraz z różnicami między protokołami dostępu do medium i samymi medianami transmisyjnymi (w sieciach lokalnych wykorzystywane są wspólne, często rozsiewcze media transmisyjne, zaś w sieciach rozległych mamy zazwyczaj do czynienia z podsiecią komunikacyjną z połączeniami typu punkt-punkt).

### 9.3 Urządzenia pośredniczące w łączaniu sieci

*Bezpośrednie łączenie sieci komputerowych dokonywane jest za pośrednictwem bądź specjalizowanych urządzeń (ang. Internetworking Units - IU), bądź też komputerów pełniących, obok różnorodnych funkcji usługowych, również i funkcje pośrednictwa we współpracy dwóch lub większej liczby sieci.*

W zależności od konkretnych potrzeb, do łączenia sieci używa się różnych typów urządzeń. W kontekście modelu OSI można mówić o łączaniu na różnych poziomach architektury warstwowej sieci. Łączenie na poziomie warstwy N wskazuje, że element łączący dwie sieci posiada moduły protokołów warstw od 1 do N obu sieci. Protokoły te mogą, choć nie muszą, być wspólne dla obu sieci.

Korzystając z modelu odniesienia ISO-OSI zdefiniować można kilka typów urządzeń pośredniczących przy współpracy sieci komputerowych - w zależności od zestawu warstw implementowanych w tych urządzeniach. Klasyfikację urządzeń IU prezentuje rysunek 9.6. Klasyfikacja ta obejmuje szereg urządzeń pośredniczących, począwszy od prostych układów sprzętowych warstwy fizycznej, jakimi są retransmitery/regeneratory (ang. repeaters), poprzez mosty (ang. bridges) i koncentratory/przełączniki (ang. hubs/schwinging hubs/schwitchens), tj. inteligentne urządzenia warstwy łączącej danych, routery (ang. routers), czyli urządzenia implementujące funkcje warstw od 1 do 3, a na bramach (ang. gateways), nazywanych też śluzami bądź konwerterami protokołów (ang. protocol converters), kończąc.



Rys. 9.6. Urządzenia sprzągające systemy komputerowe w odniesieniu do modelu ISO/OSI

*Dokonując wyboru urządzenia sprzągającego należy w pierwszej kolejności odpowiedzieć sobie na kilka istotnych pytań:*

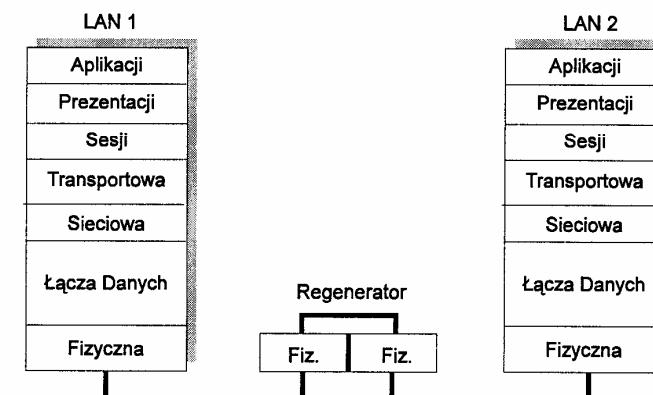
#### 9.3.1 Regeneratory i proste urządzenia przełączające

- jak duża ma być realizowana sieć;
- czy w przyszłości ma ona współpracować z sieciami rozległymi;
- czy ma ona współpracować z systemami aplikacji multimedialnych, które wymagają bardzo dużych przepustowości;
- jak drogie mogą być zastosowane urządzenia?

W kolejnym kroku należy spojrzeć na możliwości różnych urządzeń pośredniczących i dokonać stosownego wyboru, spośród bardzo dużego asortymentu produktów sieciowych dostępnych na rynku. Najważniejszymi parametrami urządzeń sprzągających są przy tym: szybkość pracy, skalowalność, obsługa różnego typu protokołów wyboru trasy, obsługa pakietów różnych protokołów sieciowych i transportowych, łatwość zarządzania wykonywanego z centralnego miejsca, jak i zarządzania zdalnego.

### 9.3.1 Regeneratory i proste urządzenia przełączające

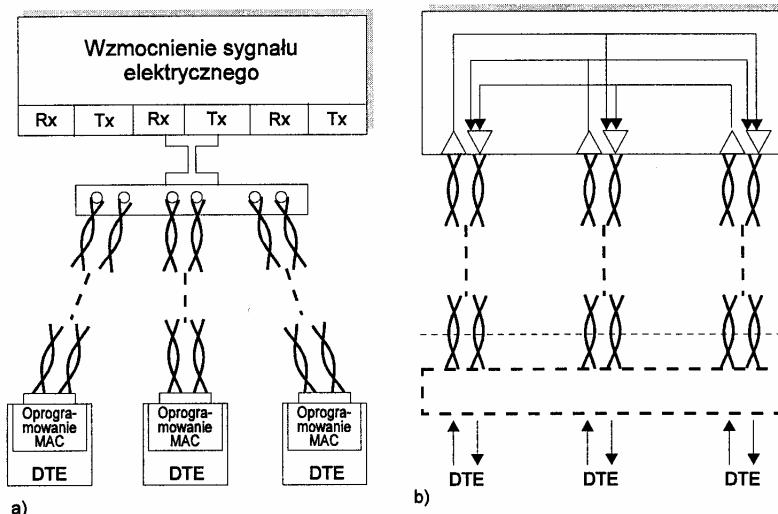
*Regeneratory, czy też retransmitery są prostymi dwuportowymi urządzeniami działającymi w warstwie fizycznej (patrz rysunek 9.7) i pozwalającymi na łączenie sieci o jednakowych standardach MAC i LLC oraz o tych samych typach mediów i identycznych szybkościach transmisji.* Regeneratory nie interpretują znaczenia retransmitowanych przez siebie sygnałów. Dokonują one jedynie regeneracji odbieranych sygnałów (przywracając im początkowe wartości poziomów napięć, częstotliwości i faz, częstotliwości i długości czasów trwania, itp.) i retransmisię tych sygnałów z jednego segmentu sieci do drugiego. Fakt ten ogranicza zastosowanie tych układów do łączenia sieci tego samego rodzaju. Przy pomocy regeneratora można więc połączyć ze sobą np. dwie sieci Ethernet, ale już połączenie sieci Ethernet z siecią Token Ring jest niemożliwe.



Rys. 9.7. Regenerator

małną długość pojedynczego segmentu, zależną między innymi od tłumienia i wnoszonych do sieci zniekształceń. Ponieważ retransmitery wprowadzają dodatkowe opóźnienia w propagacji sygnału, liczba segmentów sieci jakie mogą być przy ich pomocy łączone, jest ograniczona.

Stosowanie regeneratorów umożliwia nie tylko powiększanie zasięgu sieci, ale także zapewnia izolację elektryczną poszczególnych jej segmentów. W przypadku sieci Ethernet, uszkodzenie kabla w jednym z segmentów, połączonych przy pomocy regeneratorów, nie blokuje pracy pozostałych sprawnych fragmentów sieci. Regeneratory mają prostą konstrukcję, a w związku z tym ich cena jest stosunkowo niska. Budowa i zasada działania regeneratora zostały pokazane na rysunkach 9.8a i 9.8b.

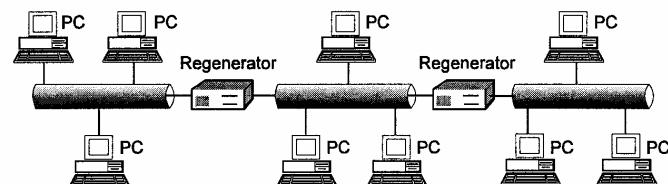


Rys. 9.8. Regenerator sygnału elektrycznego przesyłanego pomiędzy dwiema stacjami końcowymi: a) budowa retransmitera, b) schemat działania

Regeneratory są stosowane wyłącznie do rozbudowy sieci LAN. Dzięki nim można przesyłać sygnały na odległości większe niż narzucone przez specyfikację pojedynczej sieci. W opisach poszczególnych standardów określa się zwykle maksymalną rozległość sieci, w przypadku użycia regeneratorów. W zależności od standardu sieci komputerowej, wg klasyfikacji IEEE serii 802.X, retransmitery mogą być umieszczane w ścisłe określonych miejscach sieci. Przykładami najpopularniejszych retransmiterów są urządzenia wykorzystywane przy rozbudowie standar-dowych sieci IEEE 802.3 bądź sieci Ethernet - w ramach narzuconych przez te standardy maksymalnych wymiarów sieci.

### **Regeneratory w sieci Ethernet**

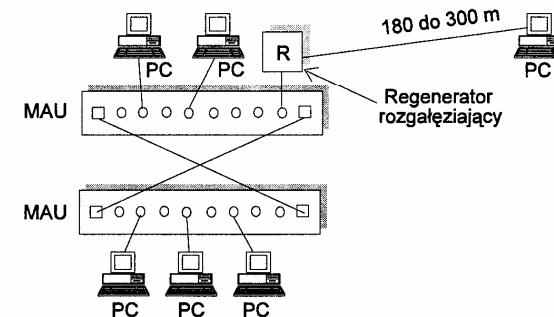
Użycie regeneratorów w sieci Ethernet jest stosunkowo proste, gdyż są one w niej stosowane standardowo do łączenia segmentów magistrali. Regenerator jest traktowany jako jeden z węzłów, w każdym z przyłączonych do niego segmentów (patrz rysunek 9.9). Ponieważ regenerator nie stanowi zakończenia magistrali, do końca kabla musi być każdorazowo podłączony terminator. Maksymalna długość pięciu połączonych retransmiterami segmentów sieci IEEE 802.3 nie powinna przekroczyć 2,5 km. W odniesieniu do sieci Ethernet dopuszcza się nieco większą długość rozbudowywanej sieci, która z uwzględnieniem 50 metrowej długości kabli pomiędzy retransmiterami a sprzęgami sieciowymi nie powinna być większa od 2,8 km.



Rys. 9.9. Przykładowe zastosowanie regeneratorów sygnałów elektrycznych w sieci standardu IEEE 802.3

### **Regeneratory w sieci Token Ring**

W sieci Token Ring stacje mogą być oddalone od układu dostępu (MAU) do 100 metrów, w przypadku skrętki nieekranowanej, bądź 200 metrów, w przypadku skrętek ekranowanych lub światłowodów. Również i przy rozbudowie sieci IBM Token Ring/IEEE 802.5 korzysta się często z regeneratorów. Normy IBM definiują maksymalną liczbę regeneratorów w pętli, w zależności od typu okablowania. Regeneratory w sieciach IBM mogą być instalowane bezpośrednio w kablu bądź, co jest bardziej typowe, w układach MAU.



Rys. 9.10. Regenerator R rozgałęziający w sieci Token Ring

W sieciach Token Ring są stosowane trzy rodzaje regeneratorów: regeneratory "Token Ring", rozgałęzające i łączące. Regenerator "Token Ring" służy do zwiększenia odległości między jednostkami MAU do ponad 300 m. Z kolei regenerator rozgałęzający wzmacnia tylko sygnały przesypane do jednego odgałęzienia, a nie całej sieci (patrz rysunek 9.10). Spośród ośmiu węzłów, które mogą być przyłączone do jednostki MAU, dowolna ich liczba może używać regeneratorów rozgałęzających. Pozwalają one zwykle podwoić standardową długość medium, dzięki czemu odległy węzeł może być przyłączony do jednostki MAU, a zatem i sieci Token Ring.

Regeneratorы łączące wzmacniają sygnały przesypane między hubami (zbudowanymi z kilku jednostek MAU), pozwalając zazwyczaj dwukrotnie zwiększyć dopuszczalną odległość między jednostkami MAU.

#### Regeneratorы w sieci Token Bus

Innym, standardowym rozwiązaniem dla sieci LAN jest Token Bus, czyli IEEE 802.4 (ISO 8802-4). W rozwiązaniu jednokanałowym (pasmowym) tej sieci pojedynczy segment może mieć długość do 1 km, pozwalając na dołączenie do niego 30 stacji końcowych (przy czym odległość stacji od kabla może wynosić do 30 metrów). Zasięg sieci, również i w tym przypadku można zwiększyć stosując urządzenia retransmisyjne (regeneratorы).

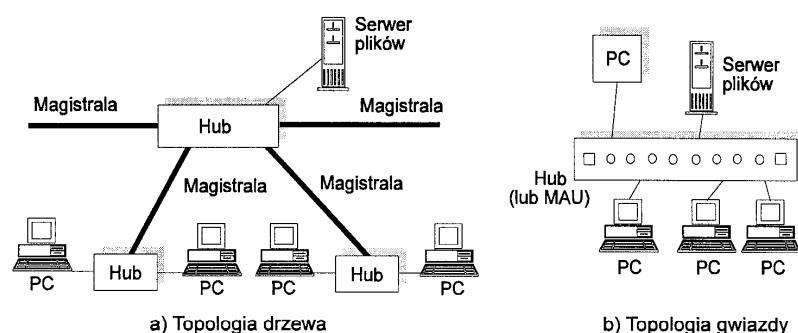
#### Huby (koncentratory)

Zadania podobne do realizowanych przez regeneratorы wypełniają też popularne huby, które można traktować jako wieloportowe regeneratorы. *Huby pełnią funkcje koncentratorów, łączących urządzenia sieciowe, przy czym połączenie to jest realizowane na poziomie medium transmisyjnego. Wyróżnia się huby aktywne i pasywne. Hub aktywny, oprócz funkcji łączenia kabli, regeneruje sygnał (podobnie jak regenerator), co istotnie zwiększa zasięg transmisji. Hub pasywny jedynie łączy kable ze sobą.* Zadaniem hubów jest, podobnie jak regeneratorów, odbieranie sygnałów z jednej stacji i przesłanie ich, bez zmian, do kilku lub kilkunastu innych stacji (wykrywanie kolizji realizowane jest w tym przypadku przez karty sieciowe w stacjach roboczych). Huby te, zwane często hubami pierwszej generacji, nie wspierają żadnych protokołów zarządzania (takich jak SNMP - ang. *Simple Network Management Protocol*). Są jednak ciągle bardzo popularne na rynku i znajdują dość powszechnie zastosowanie w małych sieciach lokalnych, a administratorzy sieci mają, dzięki nim, możliwość łatwego rozbudowywania sieci poprzez łączenie hubów między sobą.

Zastosowanie hubów ogranicza konieczność rozprowadzania kabli sieciowych po całym budynku. Konsekwencją użycia tego typu urządzeń jest zwykle zmiana fizycznej topologii sieci z magistrali lub pierścienia na gwiazdę, przy zachowaniu logicznych charakterystyk sieci. Centralne położenie huba poprawia przepustowość sieci oraz ułatwia zarządzanie siecią, w szczególności jej rekonfiguracją.

Huby mogą współpracować z sieciami typu Ethernet i Token Ring oraz z mostami i routerami.

W topologii magistralowej funkcje huba (koncentratora) spełnia, w znacznym stopniu, fragment okablowania. W topologii gwiazdy, pierścienia lub gwiaździsto-pierścieniowej, hub jest centralnym elementem, który zapewnia komunikację pomiędzy stacjami roboczymi i serwerami. Informacje docierające do sieci lub wychodzące z niej są kierowane poprzez hub do miejsca przeznaczenia. Przykładowe zastosowania hubów w sieciach o topologii drzewa oraz gwiazdy pokazuje rysunek 9.11.



Rys. 9.11. Hub w sieciach o topologii drzewa i gwiazdy

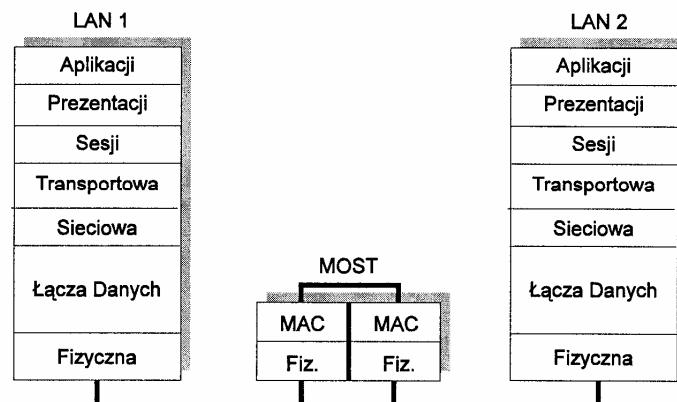
Warto zwrócić uwagę, że często pod pojęciem "huba" producenci oferują urządzenia, które nie tylko są wyposażone w kilka magistral obsługujących różne typy mediów transmisyjnych, ale mają również wbudowywane dodatkowe moduły realizujące funkcje mostów i/lub routerów oraz moduły przełączników ATM. Niektóre huby mogą dodatkowo zarządzać konfiguracją sieci i zbierać dane o jej funkcjonowaniu, co znacznie odróżnia je od prostych urządzeń typu regeneratora lub koncentratora. Dzięki swoim licznym "umiejętnościom" nazywane są one wówczas "hubami inteligentnymi". Produkowane obecnie huby inteligentne skupiają jedną lub więcej arterii osiowych (ang. *backbones*) w jednym centralnym urządzeniu. Stąd zaliczenie huba do określonej kategorii urządzeń pośredniczących powinno poprzedzić analiza wypełnianych przez niego zadań.

#### 9.3.2 Mosty

Most nazywany potocznie "brydżem" (od ang. *bridge*) jest układem łączącym identyczne lub różne sieci LAN, pozwalając tym samym na tworzenie większych, tzw. rozszerzonych sieci LAN. Współpracujące ze sobą sieci muszą mieć przy tym zaimplementowane identyczne sieciowe systemy operacyjne (ang. *Network Operating System - NOS*).

### 9.3.2.1 Koncepcja pracy mostów

W celu uzyskania zgodności pracy protokołów komunikacyjnych i wybranych aplikacji sieciowych, **mosty realizują szereg skomplikowanych czynności związanych z funkcjonowaniem warstw: fizycznej i łącza danych, a pozornie nawet warstwy sieciowej, dokonując uproszczonego routingu ramek**. W odróżnieniu od regeneratora most posiada zwykle więcej niż dwa porty. Podstawą działania mostu jest zasada "zapamiętaj i wyślij". Prowadzi on na słuch tego, co dzieje się w podłączonych do niego sieciach i retransmituje informacje między sieciami. Most nie zmienia postaci ramek, za wyjątkiem tzw. mostów tłumaczących (ang. *translating bridges*), zwykle z tzw. źródłowym wyborem trasy. Prowadzi jednak ich selekcję, tzn. retransmituje jedynie ramki skierowane do stacji zlokalizowanych na innych portach, bądź ramki do nieznanych stacji, a także ramki z adresem rozgłoszeniowym. Rysunek 9.12 prezentuje miejsce mostu w modelu ISO-OSI.



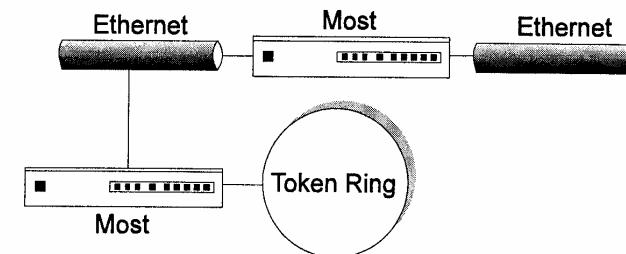
Rys. 9.12. Most

Z uwagi na integrację sieci LAN w warstwach fizycznej i łącza danych, mosty wymagają spójnego i jednoznacznego systemu adresacji (adresów MAC-owych ramek). Pożądane jest też zapewnienie identycznych formatów ramek akceptowanych we wszystkich segmentach "rozległej" sieci LAN. Mosty dokonują bowiem filtracji ramek (wg. adresów MAC-owych). Mogą też realizować stosowną konwersję pól ramek (mosty tłumaczące) bądź ich emulację oraz wyznaczać nowe sumy kontrolne.

Ponieważ **mosty łączą segmenty sieci lub też niezależne sieci LAN**, więc niejako automatycznie realizują funkcje regeneratorów. Posiadają jednak wiele zalet w porównaniu z regeneratorami i prostymi hubami. **Potrafią "uczyć się" położenia stacji w sieciach, dzięki czemu mogą odfiltrowywać ruch lokalny, przesyłany**

wewnątrz sieci, a retransmitować tylko ruch międzysieciowy.

Filtrowanie jest bardzo ważną cechą odróżniającą most od regeneratora. Dzięki niemu, ruch odbywający się między stacjami znajdującymi się w tym samym segmencie sieci nie jest przenoszony do innych segmentów, zmniejszając w ten sposób całkowite obciążenie sieci. **Most pozwala także na realizację (utrzymywanie) alternatywnych (zapasowych) połączeń między sieciami.** W momencie, gdy jedno z połączeń zostaje uszkodzone, most automatycznie kieruje ruch trasą dodatkową. Most potrafi łączyć sieci, w których zastosowano różne technologie warstwy fizycznej i różne podwarstwy MAC, dopuszczając np. łączenie sieci Ethernet i Token Ring. By połączenie to mogło funkcjonować, konieczne jest zastosowanie w obu sieciach takich samych protokołów w warstwach wyższych. Przykład tego rodzaju połączeń pokazano na rysunku 9.13, gdzie jeden most łączy dwie sieci Ethernet, a drugi - sieci Ethernet i Token Ring. Przy retransmisji ramek między różnymi technologicznie sieciami, most dokonuje między nimi automatycznej konwersji ramek MAC.



Rys. 9.13. Zastosowanie mostów do łączenia różnych typów sieci LAN

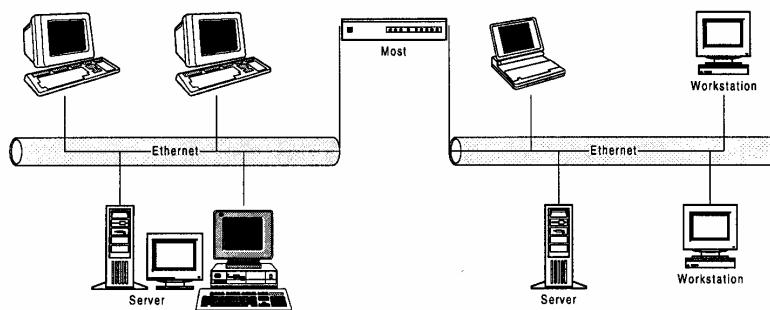
W przypadku łączenia sieci LAN brak jest jednoznacznych wymagań na stosowanie mostów. Poszczególni producenci tego typu sprzętu podają różne parametry dotyczące możliwości rozbudowy sieci LAN w oparciu o wytwarzane przez nich urządzenia. Np. mosty typu DEC LAN Bridge 100 pozwalają na łączenie sieci Ethernet w tzw. supersieci o długościach do 22 km z liczbą stacji sięgającą 8000.

**Jednym z podstawowych parametrów mostu jest jego wydajność, tj. liczba ramek obsługiwanych w jednostce czasu. Najnowocześniejsze rozwiązania mostów mogą obsługiwać do kilkudziesięciu tysięcy ramek w czasie jednej sekundy.**

Reasumując, poza możliwością rozbudowy sieci, do wymiarów nieosiągalnych przy zastosowaniu regeneratorów, można wymienić szereg innych ważnych przy czyn stosowania mostów. Są to między innymi:

- Możliwość łączenia sieci LAN o odmiennych technologiach warstwy fizycznej. Z tego względu mosty są często wykorzystywane do łączenia różnych typów podsieci LAN, tj. systemów pasmowych, szerokopasmowych względnie systemów z transmisją w paśmie podstawowym;

- Możliwość łączenia sieci LAN o odmiennych standardach warstwy MAC. Mosty modyfikują wówczas formaty ramek do postaci obowiązującej w każdej z łączonych sieci (mosty realizujące łączenie sieci o odmiennych standardach LAN wyposażone są w układy szybkiej konwersji i/lub emulacji pól ramek). Mosty tego typu określane są mianem mostów tłumaczących;
- Możliwość separacji ruchu w sieci przez jej podział na mniejsze fragmenty. W przypadku dużego ruchu generowanego lokalnie i/lub kierowanego do kilku serwerów sieci LAN, prawidłowy podział sieci na mniejsze "domeny kolizyjne", obejmujące grupy stacji i związane z nimi serwery, powoduje radykalne zmniejszenie obciążenia w poszczególnych, odseparowanych mostami segmentach sieci. Wpływa to na zmniejszenie opóźnień w dostępie do medium i podniesienie jakości usług świadczonych przez sieci. Przykładowy podział sieci, z użyciem mostu, na dwie podsieci, został przedstawiony na rysunku 9.14.



Rys. 9.14. Schemat podziału sieci lokalnych przy udziale mostu

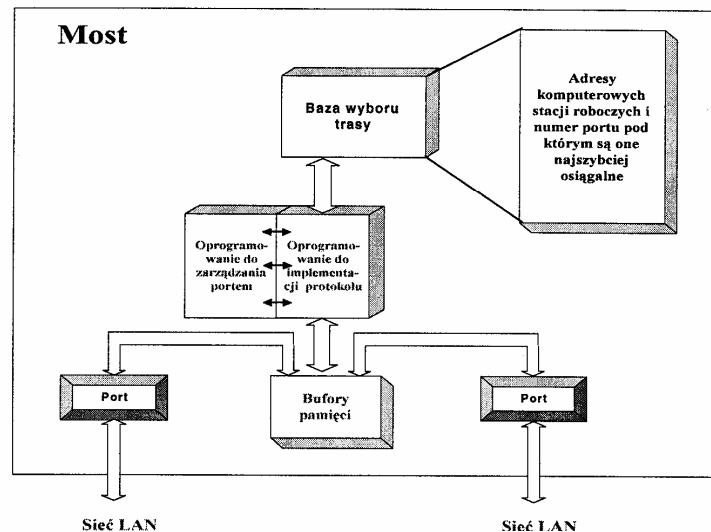
- Zdolność do filtracji ramek, pozwalająca zarówno na poprawę bezpieczeństwa pracy sieci jak też różnicowanie uprawnień w dostępie do sieci. W pierwszym przypadku most może stanowić barierę zapobiegającą rozprzestrzenianiu się stanu przeciążenia w sieci (ang. *fire wall*). W drugim przypadku most pozwala na ograniczenie dostępu do sieci określonym adresem fizycznym.

Do dodatkowych zalet mostu należy zaliczyć niewysoką cenę i łatwą konfigurację.

Najpoważniejszymi wadami mostu są:

- brak zabezpieczenia przed chwilowymi wzrostami natężenia transmisji ramek skierowanych na adres rozgłoszeniowy - tzw. sztormami ramek broadcastowych, uniemożliwiającymi pracę sieci poprzez całkowite wykorzystanie pasma transmisyjnego medium oraz
- wynikające z zasady budowy i działania mostu, wprowadzanie dodatkowych opóźnień związanych z czasem koniecznym na buforowanie

odbieranych ramek, analizą ich zawartości i badaniem ich poprawności (patrz rysunek 9.15).



Rys. 9.15. Budowa mostu przeźroczystego

Łączenie sieci o różnych protokołach podwarstwy MAC powoduje, że formaty ramek muszą być zmieniane. Wymusza to konieczność wyznaczania przez most nowych sum kontrolnych i stwarza zagrożenie, że błędy powstałe w czasie tej konwersji mogą pozostać niewykryte.

Podejmując decyzję zarówno o łączeniu sieci LAN, jak też o ich podziale na mniejsze obszary musimy uwzględnić możliwości mostu z punktu widzenia buforowania ramek jak i szybkości ich obsługi. W przypadku źle zaprojektowanego połączenia sieci LAN most może bowiem stać się wąskim gardłem sieci. Dotyczy to głównie łączenia segmentów sieci o różnych szybkościach pracy.

Z uwagi na znaczenie mostu jako podstawowego układu łączącego sieci LAN, w dalszej części rozdziału zaprezentujemy nieco rozszerzoną klasyfikację i opis wybranych typów mostów.

### 9.3.2.2 Typy mostów

Opracowanie przez podkomitet IEEE 802.5 dla sieci typu Token-Ring, efektywnego mechanizmu wyboru trasy ramki - przez stację źródłową - określonego mianem routingu źródłowego (ang. *source routing*), spowodowało w konsekwencji wyodrębnienie się dwóch odmiennych koncepcji pracy mostów. Pierwsza z nich odnosi się do mostów pracujących w oparciu o algorytm drzewa opinającego (ang.

*Spanning Tree*). Mosty te same podejmują decyzje o wyborze trasy i przekazują ramki do odbiorcy dokładnie w takiej postaci, w jakiej zostały one przygotowane przez nadawcę. Stąd też powszechnie przyjęta nazwa tego rodzaju mostów, to **mosty transparentne lub przeźroczyste** (ang. *transparent bridges*). Mosty przeźroczyste, opracowane przez firmę DEC, uznane zostały za standard IEEE oznaczany symbolem 802.1d. Standard ten jest powszechnie stosowany do sprzęgania sieci korzystających z protokołów dostępu CSMA/CD i Token Bus.

W drugim, wspomnianym na wstępie, typie mostów z routingiem źródłowym, funkcje obsługi ramek ograniczają się do śledzenia i wyboru właściwej trasy przesyłania ramki zdefiniowanej przez stację źródłową. Informacja routingowa składa się przy tym z numerów: segmentów sieci LAN i mostów, przez które ramka ma być przesłana. Z tej racji **mosty takie nazywane są source-routingowymi czyli ze sterowaniem źródłowym**. Mosty tego typu mogą być w zasadzie użyte do łączenia wszystkich typów sieci lokalnych (dzięki wprowadzeniu do ramki opcji definiującej jej transparentne traktowanie przez most). Niektórzy autorzy nie uwzględniają jednakże tej poprawki i wtedy mosty ze sterowaniem źródłowym mogą łączyć jedynie sieci typu Token Ring. Standaryzacją tego typu mostów zajął się komitet IEEE 802.5.

W praktyce używane są również **mosty łączone**, tzn. **source routingowe transparentne (SRT)**, które pracują jako mosty przeźroczyste dla ruchu „transparentnego” z sieci Ethernet lub Token Bus oraz jako mosty source routingowe dla ramek zawierających pole „Source Routing”.

Aby o danym urządzeniu można było mówić iż jest to most, musi ono spełniać szereg warunków i realizować szereg funkcji. Podstawowe funkcje i warunki konieczne definiujące most przeźroczysty zostały zawarte w standardzie IEEE 802.1d.

### 9.3.2.3 Podstawowe funkcje mostów przeźroczystych

Most powstał jako urządzenie mające umożliwić, w wielu sprężonych ze sobą sieciach lokalnych, poprawną realizację aplikacji, przygotowanych pierwotnie dla pojedynczej sieci LAN. Zadaniem mostu jest więc takie połączenie sieci (najczęściej lokalnych), by z punktu widzenia dołączonych do nich stacji sieciowych stanowiły one pojedynczą i jednorodną sieć.

By móc pełnić swoją rolę, każdy most powinien potrafić realizować pewien podstawowy zestaw funkcji. Są to:

- nasłuch transmisji w dołączonych do mostu sieciach i umiejętność retransmisji odbieranych ramek,
- umiejętność uczenia się położenia stacji sieciowych na podstawie generowanego przez nie ruchu,
- realizacja algorytmu bezpetlowego drzewa opinającego (ang. *Spanning Tree*).

Most realizujący wszystkie powyższe funkcje nazywany jest mostem przeźroczystym. Nazwa ta wynika z faktu, iż w żaden sposób nie modyfikuje on retransmitowanych przez siebie ramek i jest w zasadzie niewidoczny dla stacji końcowych. Umiejętność retransmisji otrzymanej informacji jest podstawową funkcją, która musi być zaimplementowana w moście, by można było mówić o łączeniu sieci. Most realizuje tę funkcję odbierając wszystkie ramki transmitowane we wszystkich dołączonych do niego sieciach, i gdy jest to konieczne, retransmitując odebrane ramki do innych sieci. Mówiąc, że most działa według zasady “zapamiętaj i prześlij”. By ramka mogła być retransmitowana (przesłana), musi być wcześniej w całości odebrana (zapisana do pamięci mostu).

Uczenie się położenia stacji sieciowych jest inną, istotną funkcją mostu. Pozwala ona bowiem na ograniczenie ruchu w dołączonych sieciach. Dzięki temu most jest w stanie odróżnić ruch lokalny, wewnętrz dołączonego segmentu LAN, który nie musi być retransmitowany do innych segmentów, od ruchu międzymiesięcowego, który powinien być retransmitowany między komunikującymi się sieciami.

Podstawowym problemem przy łączeniu sieci, przy pomocy mostów, jest możliwość krajienia ramek w sieci. W celu zapobieżenia temu zjawisku, w mostach przeźroczystych realizowana jest ostatnia z w/w funkcji, czyli funkcja tworzenia drzewa opinającego gwarantującego brak pętli. Dzięki algorytmowi Spanning Tree zespół mostów potrafi sam doprowadzić do zablokowania tworzących pętle połączeń, realizując tym samym topologię bezpetlową.

### 9.3.2.4 Klasyfikacja mostów przeźroczystych

Zaprezentowana w niniejszym podrozdziale klasyfikacja ma na celu zilustrowanie podstawowych zasad pracy mostu, z uwzględnieniem jego głównych bloków funkcjonalnych. Opisane dalej, kolejne warianty mostu przeźroczystego, tj. most przeźroczysty prosty i most przeźroczysty uczący się, nie są w rzeczywistości realizowane. Ich opis stanowi jedynie próbę kilku etapowej konstrukcji funkcji pełnego mostu przeźroczystego i zwrócenie uwagi na podstawowe zjawiska zachodzące w moście i w dołączonych do niego sieciach.

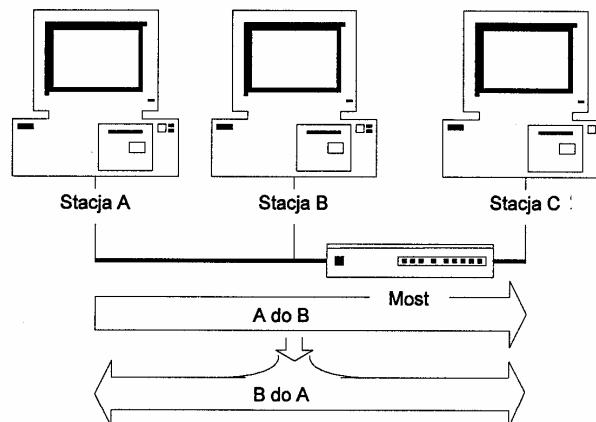
#### 9.3.2.4.1 Most przeźroczysty prosty

Zadaniem prostego mostu przeźroczystego jest integracja odrębnych sieci LAN, a tym samym zapewnienie wymiany informacji między poszczególnymi sieciami. Przekazywane ramki nie powinny być przy tym modyfikowane. Ramka retransmitowana powinna więc wyglądać dokładnie tak samo jak ramka oryginalnie nadana przez nadawcę.

Nawet tak proste urządzenie jak most pozwala na zniesienie kilku ograniczeń narzuconych przez pojedyncze sieci lokalne. W szczególności zastosowanie mostu przeźroczystego prostego pozwala na powiększanie rozmiarów sieci, w większej znacznie skali niż umożliwiają to regeneratorы, a w sieciach Token Ring pozwala na pokonanie ograniczenia liczby stacji znajdujących się w pojedynczym pierścieniu.

Nie sposób jednak nie zwrócić uwagi na oczywiste wady stosowania mostów. W stosunku do regeneratora, zmieniane są znacznie charakterystyki czasowe połączonych sieci. Regenerator retransmituje z niewielkim opóźnieniem wszystkie kolejne bity informacji. Most natomiast, by mógł retransmitować ramkę, musi ją wcześniej w całości odczytać. Problem ten jest niestety typowy dla wszystkich urządzeń pracujących według zasady "zapamiętaj i prześlij". Pewnym rozwiązaniem problemu opóźnień jest zastosowanie technologii przełączania pakietów określane mianem "cut-through". W technologii tej, ramka kierowana jest do właściwego portu tak szybko jak to jest możliwe, czyli natychmiast po odczytaniu adresu przeznaczenia MAC, zmniejszając tym samym znacznie wprowadzaną opóźnienie.

Inną wadą mostu przeźroczystego prostego jest fakt, iż nie wszystkie ramki odebrane z dołączonych do mostu sieci wymagają retransmisji. W przedstawionej na rysunku 9.16 sytuacji, przy zastosowaniu opisanego wcześniej mostu prostego, ruch przeznaczony dla znajdujących się w tym samym segmencie sieci stacji (stacje A i B) zostanie niepotrzebnie przesyłany do segmentu sieci, w którym znajduje się stacja C.



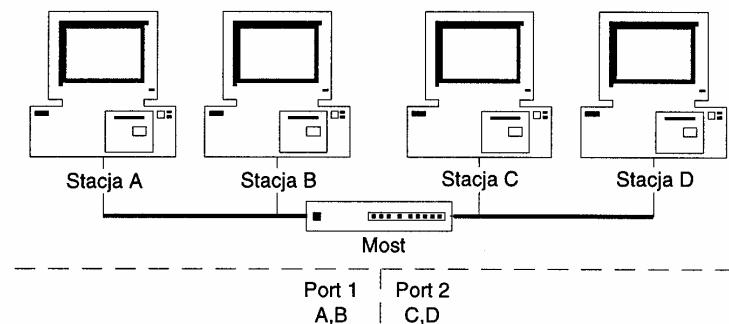
Rys. 9.16. Ruch lokalny między stacjami A i B przenoszony do drugiego segmentu sieci przez most transparentny prosty

Istnieje jednak bardzo proste rozwiązanie powyższego problemu - most powinien uczyć się położenia stacji sieciowych.

#### 9.3.2.4.2 Most przeźroczysty uczący się

Przykład zaprezentowany na rysunku 9.16 pokazuje jak niekorzystne, z punktu widzenia obciążenia sieci, jest niepotrzebne retransmitowanie ramek. Istnieje jednak prosta metoda zapobieżenia temu zjawisku - wystarczy, by most wiedział, które

stacje sieciowe widziane są przez poszczególne porty i nie retransmitował ramek do tych portów, przez które nie jest osiągalna stacja przeznaczenia ramki. Ponieważ wszystkie stacje w sieci lokalnej posiadają swoje, unikatowe w skali sieci, identyfikatory - adresy MAC, wykorzystywane w transmitowanych ramkach, most jest w stanie, w prosty sposób, podejmować decyzje, które ramki mają być retransmitowane, a które nie.



Rys. 9.17. Most znający położenie stacji w sieci

Na rysunku 9.17 przedstawiony został przykład, w którym most zna położenie stacji w sieci. W tej sytuacji, gdy na porcie nr 1 otrzyma on ramkę przeznaczoną dla stacji D, to wiedząc, że stacja ta jest osiągalna na porcie nr 2 retransmituje tam usłyszaną ramkę. Z kolei otrzymując na porcie nr 1 ramkę przeznaczoną dla stacji A, to wiedząc, że stacja ta jest obsługiwana przez port nr 1 nie przekaże tej ramki dalej. W ten sposób ruch lokalny, generowany i adresowany wewnątrz segmentów sieci, nie "przenika" do innych segmentów, zmniejszając tym samym obciążenie sieci.

Skąd jednak most ma czerpać wiedzę o położeniu stacji? Do tego celu wykorzystywany jest adres nadawcy, znajdujący się w każdej ramce transmitowanej przez sieć. Wykorzystując tę informację, most potrafi automatycznie gromadzić wiedzę o położeniu stacji.

Algorytm działania mostu uczącego się można opisać następująco:

1. Most odbiera wszystkie ramki pojawiające się na wszystkich portach.
2. Dla każdej odebranej ramki zapamiętuje adres nadawcy wraz z numerem portu, przez który ramka została odebrana i czasem jej odbioru.
3. Dla każdej odebranej ramki most porównuje adres przeznaczenia z adresami już zapamiętanymi i:
  - gdy adres nie był jeszcze „słyszany” na żadnym z portów, retransmituje ramkę na wszystkie porty, z wyjątkiem tego, z którego została odebrana,

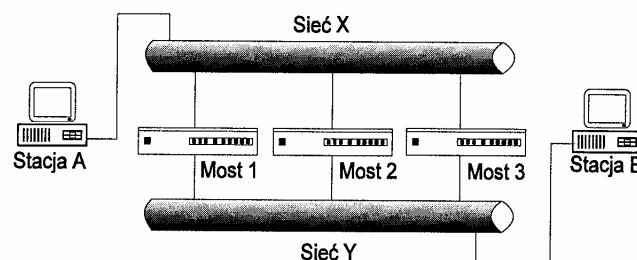
- gdy adres był już „słyszany”, ramka przekazywana jest tylko na ten port, który jest związany z danym adresem, a gdy jest to port, z którego ramka została odebrana, most usuwa ją bez retransmisji (takie działanie mostu nazywane jest filtrowaniem ramek).
4. Most okresowo przegląda zapamiętane adresy i usuwa te, które odebrane zostały “zbyt dawno”.

Dzięki powyższym procedurom most stopniowo dowiaduje się, jakie stacje są osiągalne na poszczególnych portach i filtryuje ruch lokalny. Z kolei zastosowanie mechanizmu time-out'ów i usuwania długo nie używanych adresów pozwala na utrzymywanie rozmiaru bazy danych na założonym poziomie.

Powyższy schemat działania mostu ma pewną wadę. Zakłada on mianowicie, iż stacja która otrzymuje informacje z sieci, sama też okresowo wysyła dane. Może to prowadzić do przeterminowania zapisu o położeniu danej stacji i w efekcie do niepotrzebnego rozprzestrzeniania się po sieci ramek przeznaczonych dla np. stacji wyłączonej.

Most uczący się ma też i inną poważną wadę - w katastrofalny dla sieci sposób reaguje on na pętle w sieci. Rozwiązańem tego problemu jest zastosowanie algorytmu drzewa opinającego, gwarantującego bezpłotowe struktury sieci LAN.

#### 9.3.2.4.3 Most z algorytmem drzewa opinającego



Rys. 9.18. Ilustracja problemu pętli w sieciach połączonych mostami

Przedstawiony w poprzednim podpunkcie most uczący się, mimo swoich zalet, posiadał też kilka poważnych wad, prowadzących do nieefektywnego wykorzystania sieci, a nawet uniemożliwiających ich poprawną pracę. Na 9.18 przedstawiona została sytuacja, w której dwie sieci X i Y połączone są za pomocą trzech mostów. Założymy, że w sieci X stacja A nadaje ramkę do stacji B, o której mosty jeszcze nic nie wiedzą (tj. nie znają jej położenia). W takiej sytuacji wszystkie trzy mosty prześlą otrzymaną ramkę do sieci Y - w sieci tej znajdą się więc trzy kopie ramki pochodzącej od stacji A. Następnie każdy most odbierze dwie kopie ramki z sieci Y i przekaże je z powrotem do sieci X. Sytuacja taka jest bardzo niebezpieczna, ponieważ ramki nie tylko krążą bez końca, lecz ich liczba ulega

#### 9.3.2 Mosty

zwielokrotnieniu (w powyższym przykładzie, po każdym przejściu liczba ramek wzrasta dwukrotnie). Sytuacja ta prowadzi, w bardzo krótkim czasie, do zajęcia przez retransmitowane ramki poważnej części pasma sieci X i Y, a także do przepełnienia buforów mostów i, tym samym, zablokowania ich normalnej pracy.

Rozwiązańem tego problemu jest wyeliminowanie z procesu retransmisji tych portów mostów, które retransmitując ramki pozwalały na ich krążenie między mostami. *Dla uniemożliwienia krążenia ramek w połączonych mostami sieciach, komitet IEEE 802 zaproponował realizację, przez mosty, tzw. algorytmu drzewa opinającego* (ang. *Spanning Tree*). *Algorytm ten gwarantuje utworzenie „bezpieczeństwowej topologii” sieci dla przesyłanych ramek.* Mówiąc o bezpieczeństwowej topologii (odpowiadającej topologii drzewa) mamy na myśli określony układ aktywnych (przepuszczających ramki informacyjne) i zablokowanych (nie dopuszczających do przesłania ramek informacyjnych) portów mostów, a nie topologii fizycznej sieci. Zadaniem algorytmu Spanning Tree jest więc włączanie i wyłączenie pewnych portów mostów dla ramek informacyjnych.

Realizacja algorytmu wiąże się z periodyczną wymianą między mostami specjalnych informacji (komunikatów konfiguracyjnych), zwanych jednostkami danych protokołu mostu BPDU (ang. *Bridge Protocol Data Unit*). Informacje te umożliwiają wyznaczanie portów i połączeń koniecznych do zablokowania w celu uniknięcia pętli. W każdym BPDU znajdują się informacje potrzebne by:

- Mosty wybrały spośród siebie most będący korzeniem drzewa (ang. *root bridge*);
- Każdy most wyznaczył długość najkrótszej drogi od siebie do korzenia;
- Dla każdej sieci lokalnej został wyznaczony jeden most (ang. *designated bridge*), znajdujący się najbliżej mostu-korzenia. Wyznaczony most będzie odpowiedzialny za przekazywanie ramek z tej części sieci w kierunku mostu korzenia;
- Każdy most wybrał pojedynczy port (ang. *root port*), przez który odbierane będą retransmitowane ramki do mostu-korzenia. Port ten jest jednocześnie związany z najkrótszą trasą do mostu korzenia;
- Każdy most określił, które porty mają być dołączone do drzewa opinającego (powinien być to root port i wszystkie te porty, które łączą dany most z sieciami, dla których został on wybrany jako most wyznaczony - desygnowany).

Ruch danych jest zablokowany poprzez te porty, które nie zostały włączone do drzewa opinającego.

Realizacja algorytmu Spanning Tree opiera się wyłącznie na wymianie i porównywaniu ramek konfiguracyjnych BPDU. Ważną cechą algorytmu jest zatem umiejętność porównywania przez mosty poszczególnych komunikatów i ustalania ich „wagi”. Z punktu widzenia konieczności porównywania między sobą ramek BPDU istotne są cztery zawarte w nich parametry:

- identyfikator mostu-korzenia (ang. *Root ID*),
- identyfikator mostu nadającego komunikat,
- długość ścieżki do korzenia (aktualnie najkrótszej trasy znanej przez most),
- identyfikator portu, przez który komunikat BPDU został nadany.

Identyfikatory mostu - korzenia i mostu nadającego komunikat mają taką samą strukturę. Są to 8-mio bajtowe liczby, w których dwa starsze bajty mogą być zmieniane przez administratora mostu i noszą nazwę priorytetu mostu, a sześć młodszych bajtów jest zwykle adresem MAC jednego z portów (zwykle pierwszego). Każdy most posiada przy tym wewnętrzną numerację portów. Pierwszym portem jest ten, którego numer porządkowy jest najmniejszy.

Długość ścieżki do korzenia jest wyznaczana jako liczba mostów znajdujących się na tej ścieżce. W komunikacie konfiguracyjnym długość ta zapisana jest jako liczba czterobajtowa.

Identyfikator portu składa się z dwu bajtów. Bajt starszy, który może być przez użytkownika zmieniany, nosi nazwę priorytetu portu. Bajt młodszy jest zwykłym kolejnym numerem porządkowym portu.

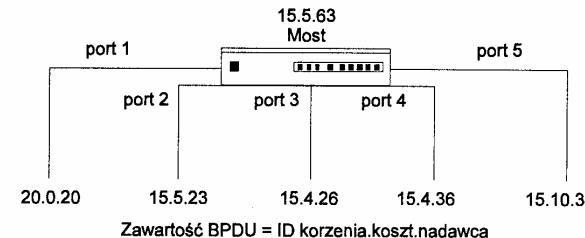
Wszystkie powyższe parametry stanowią podstawę do porównywania poszczególnych BPDU między sobą. Z dwóch BPDU, za „lepszy” uważany jest ten, w którym identyfikator mostu-korzenia jest mniejszy. Gdy identyfikatory te są równe, to „lepszy” jest ten komunikat, w którym informacja o odległości do korzenia ma mniejszą wartość. Gdy odległości są równe, „lepszym” jest ten komunikat, w którym identyfikator mostu nadawcy jest mniejszy. Gdy i te identyfikatory są równe, to ostatnią wartością różnicującą komunikaty jest identyfikator portu - mniejszy identyfikator portu wskazuje na komunikat „lepszy”.

Na początku pracy każdy z mostów uważa siebie za korzeń drzewa opinającego i zaznacza ten fakt w wysyłanych przez siebie BPDU przez ustawienie identyfikatora korzenia na swój identyfikator i ustawienie odległości do korzenia na zero. W czasie pracy, most otrzymuje komunikaty od innych mostów dołączonych do tych samych sieci i porównuje je z komunikatami, które sam by nadał do tych sieci. Jeśli komunikat otrzymany przez określony port jest „lepszy” od tego, który mógłby być nadany przez dany most, to most ten zaprzestaje nadawania BPDU przez ten port. W wyniku takiego działania, po ustabilizowaniu się algorytmu, tylko jeden most dołączany do każdej z sieci nadaje komunikaty konfiguracyjne.

Na podstawie informacji zawartych w BPDU, most podejmuje szereg decyzji dotyczących pracy swoich portów. Ustala root port, porty prowadzące do sieci, na których jest mostem wyznaczonym, a także porty, które powinny być zablokowane. Mechanizm podejmowania tych decyzji ilustruje zamieszczony poniżej przykład wyboru portów drzewa opinującego.

W przykładzie zamieszczonym na rysunku 9.19 pokazany jest most z pięcioma portami, którego identyfikator równy jest 63 (w celu uproszczenia przykładu

w BPDU nie został uwzględniony identyfikator portu). Otrzymując komunikaty konfiguracyjne BPDU na poszczególnych portach, most stale porównuje je między sobą, a także z komunikatem, który sam nadałby na danym porcie.



Rys. 9.19. Wybór portów przez most

Po zainicjowaniu algorytmu, most ustawia siebie jako korzeń (*root*) i periodycznie transmituje na wszystkich portach komunikat 63.0.63 (BPDU= identyfikator\_korzenia.koszt.nadawca). Po otrzymaniu komunikatów od innych mostów (20.0.20, 15.5.23, 15.4.26, 15.4.36 i 15.10.34) okazuje się, że najlepszy identyfikator, stanowiący tym samym identyfikator korzenia, równy jest 15 i najbliżej jest do niego przez porty 3 (15.4.26) i 4 (15.4.36). Biorąc z kolei pod uwagę identyfikatory nadawców (26 na porcie 3 i 36 na porcie 4), most 63 wybierze port nr 3 jako port wiodący do korzenia drzewa opinującego. Jednocześnie ustali swój nowy komunikat na 15.5.63, który będzie od tej pory nadawać (wartość 5 oznacza odległość mostu 63 do korzenia, tj. zwiększoną o jeden odległość od korzenia mostu 26). Ostatnią fazą wyliczeń jest porównanie przeznaczonego do nadania komunikatu (15.5.63) z otrzymanymi BPDU. Komunikaty otrzymane na portach 1 (20.0.20) i 5 (15.10.34) są gorsze i tym samym na tych portach most staje się mostem wyznaczonym. Natomiast komunikaty na portach 2 (15.5.23) i 4 (15.4.36) są lepsze od tego, który byłby nadany przez dany most o numerze identyfikacyjnym 63. Zostaną one zatem zablokowane - oznacza to, iż ruch danych zostaje na tych portach wstrzymany. Nadal będą one jednakże uczestniczyć w procedurach algorytmu Spanning Tree.

W komunikatach konfiguracyjnych znajdują się też pola określające “wiek”, czyli czas przebywania jednostek BPDU w sieci. W czasie „pobytu” jednostki BPDU w moście, zawartość pola wieku jest systematycznie zwiększana. W przypadku, gdy osiągnięta zostanie wartość maksymalna, dany komunikat BPDU jest usuwany i następuje ponowne przeliczenie stanu wszystkich portów. Dzięki temu prostemu mechanizmowi most dostosowuje się do ewentualnych zmian w topologii sieci.

Ogólnie przeliczanie (aktualizacja) stanu portów następuje w dwu sytuacjach:

- po otrzymaniu na danym porcie komunikatu BPDU lepszego od aktualnie przechowywanego, lub „posiadającego” mniejszy wiek od aktualnie przechowywanego,

- po usunięciu BPDU na skutek przekroczenia dopuszczalnego wieku komunikatu.

Podczas przełączania portów między stanami blokady i odblokowania, mosty muszą zachować szczególną uwagę ze względu na niebezpieczeństwa związane z możliwością powstania pętli w topologii. Aby zmniejszyć prawdopodobieństwo takiej ewentualności, w algorytmie Spanning Tree został przewidziany specjalny mechanizm zmiany stanu portów.

Algorytm Spanning Tree nie działa synchronicznie na wszystkich mostach. Komunikaty konfiguracyjne potrzebują nieco czasu, by poinformować wszystkie mosty o aktualnej topologii sieci. Potencjalnie, niebezpieczne jest przełączenie portu ze stanu blokady w stan odblokowania i retransmisja ramek przez ten port, ponieważ nie wszystkie mosty muszą być poinformowane o nowej topologii. Grozi to powstaniem pętli. W celu zminimalizowania prawdopodobieństwa powstania pętli, odblokowanie portu następuje po dwóch, trwających równe okresy, fazach:

- fazie nasłuchu,
- fazie uczenia się.

W pierwszej fazie, będącej fazą przejściową, port zachowuje się dokładnie tak samo jakby był zablokowany, tj. nie przekazuje ramek danych i nie uczy się położenia dołączonych do niego stacji, lecz wciąż obsługuje algorytm Spanning Tree.

W drugiej fazie port nadal nie przekazuje ramek danych, lecz uczy się już adresów „słyszanych” stacji. Dzięki temu po zakończeniu tej fazy most powinien posiadać informację o większości stacji znajdujących się w dołączonym segmencie i od razu filtrować większość ruchu.

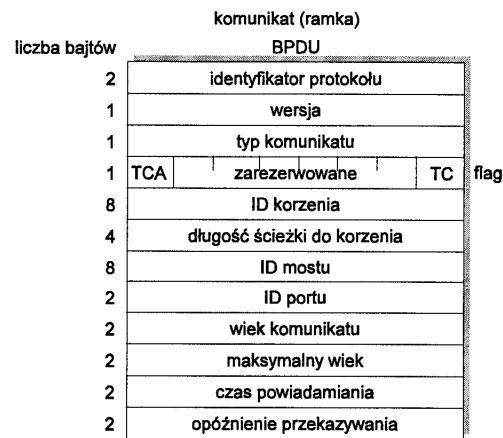
#### Parametry algorytmu Spanning Tree i format komunikatu BPDU

W algorytmie Spanning Tree istnieje szereg parametrów, na które ma wpływ administrator sieci. Parametry te obejmują:

- Priorytet mostu (ang. *bridge priority*): jest to dwubajtowa liczba, która daje administratorowi sieci możliwość wpływu na wybór korzenia drzewa opinającego. Priorytet stanowi dwa najstarsze bajty identyfikatora mostu. Im mniejszy jest ustawiony priorytet, tym większa szansa, iż most zostanie wybrany korzeniem.
- Priorytet portu (ang. *port priority*): jest to „starsza” część identyfikatora portu. Młodsza część identyfikatora jest zwykle ustalana przez oprogramowanie mostu i stanowi wewnętrzny numer portu. Administrator ma wpływ na starszą część i może tam wpisać dowolną wartość wpływając tym samym na wybór portu, który ma być zablokowany, przy wielu portach dołączonych do tej samej sieci.

- Czas powiadamiania (ang. *hello time*): jest to odstęp czasu upływający między wysłaniem kolejnych BPDU. Zalecaną wartością są 2 sekundy. Zmniejszanie tego czasu zwiększa pewność działania algorytmu w środowisku, gdzie prawdopodobieństwo zaginięcia ramek jest wysokie; z kolei zwiększanie tego czasu zmniejsza nakład pracy związany z obsługą algorytmu.
- Maksymalny wiek (ang. *max age*): jest to czas życia komunikatu BPDU, po upływie którego BPDU jest usuwany. Ustawienie zbyt małej wartości może powodować niepotrzebne rekonfiguracje topologii, natomiast ustawienie zbyt dużej wartości wpłynie na dużą bezwładność sieci przy rekonfigurowaniu. Wartością zalecaną przez standard 802.1d jest 20 sekund.
- Opóźnienie przekazywania (ang. *forward delay*): parametr ten określa długość każdego z dwu pośrednich stanów przy przejściu portu ze stanu blokady do stanu przekazywania ramek. Ustawienie tego parametru na zbyt małą wartość może spowodować powstawanie chwilowych pętli w topologii. Duża wartość powiększa natomiast czas rekonfiguracji algorytmu i wydłuża czas możliwego braku połączeń między sieciami. Opóźnienie przekazywania jest też wykorzystywane jako maksymalny wiek przechowywanych informacji o położeniu stacji w sieci w czasie zmiany topologii. Wartością zalecaną w 802.1d jest 15 sekund.
- Długi czas życia (ang. *long cache timer*): parametr ten określa czas, po upływie którego z pamięci mostu usuwane są informacje o położeniu stacji w sieci. Wartością zalecaną w 802.1d jest 5 minut.
- Koszt ścieżki (ang. *path cost*): jest to liczba dodawana do wartości odległości od korzenia, w otrzymanym na danym porcie komunikacie BPDU, w celu wyznaczenia odległości z danego mostu do korzenia poprzez określony port. Wartość ta może być ustawiana niezależnie na każdym porcie. Ustawienie dużej wartości zwiększa prawdopodobieństwo, że most stanie się „liściem” w drzewie opinującym.

Powyzsza lista przedstawia wszystkie parametry, na które wpływ ma administrator sieci. Trzy z nich, a mianowicie: czas powiadamiania, opóźnienie przekazywania i maksymalny wiek, powinny mieć taką samą wartość na wszystkich dołączonych do sieci mostach. Problem ten został rozwiązany przez umieszczenie tych parametrów w wysyłanych przez korzeń komunikatach BPDU. Każdy most otrzymujący BPDU od korzenia jest zobowiązany do wykorzystania zawartych w nim parametrów. Tym samym zmiana trzech wymienionych parametrów w moście nie będącym korzeniem nie ma wpływu na pracę algorytmu. Jednakże, gdy most ten stanie się korzeniem, to będzie on wstawił swoje wartości do BPDU i wszystkie mosty dołączone do sieci będą używać tych wartości. Format komunikatu BPDU przedstawiony jest na rysunku 9.20.



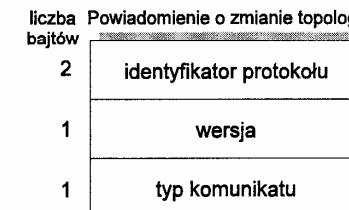
Rys. 9.20. Format komunikatu BPDU

Kolejne pola komunikatu BPDU to:

- Identyfikator protokołu: stała równa 0
- Wersja: stała równa 0
- Typ komunikatu: stała równa 0
- Flagi:
  - TC (ang. *Topology Change*), najmłodszy bit, jest to flaga zmiany topologii. Gdy wartość TC jest ustawiona w BPDU otrzymanym na root porcie oznacza to, że most ma wykorzystywać opóźnienie przesyłania (ang. *forward delay*) jako maksymalny czas przechowywania informacji o położeniu stacji w sieci, lub jako długi czas życia (ang. *long cache timer*), gdy bit ten jest wyzerowany.
  - TCA (ang. *Topology Change Acknowledgment*), najstarszy bit, jest to flaga potwierdzenia otrzymania komunikatu o zmianie topologii. Otrzymanie BPDU z root portu z ustawioną flagą TCA oznacza, że most następny na drodze do korzenia odebrał komunikat o zmianie topologii i przejął na siebie odpowiedzialność za poinformowanie o tym korzenia.
  - pozostałe bity w bajcie są niewykorzystane.
- ID korzenia: identyfikator mostu uważanego za korzeń drzewa opinającego. Identyfikator składa się z dwubajtowego pola zwanego priorytetem i sześciu bajtów identyfikatora będących zwykle adresem MAC jednego z portów mostu.
- Długość ścieżki do korzenia: całkowita długość ścieżki od mostu, który nadał dany komunikat BPDU, do korzenia identyfikowanego przez poprzedni parametr.

- ID mostu: identyfikator mostu nadającego komunikat, składający się z dwu bajtów priorytetu i sześciu bajtów identyfikatora.
- ID portu: dwubajtowa liczba. Starszy bajt jest to definiowany przez administratora priorytet portu. Młodszy bajt to numer portu, przez który dane BPDU zostało nadane.
- Wiek komunikatu: czas liczony w 1/256 częściach sekundy, wyznaczający okres, jaki upływał od nadania danego komunikatu BPDU przez most-korzeń drzewa opinującego.
- Maksymalny wiek: czas liczony w 1/256 częściach sekundy, po którym komunikat BPDU jest usuwany.
- Czas powiadamiania: okres czasu liczony w 1/256 częściach sekundy, jaki upływa pomiędzy generacją dwu kolejnych BPDU przez most-korzeń.
- Opóźnienie przekazywania: okres czasu, liczony w 1/256 częściach sekundy, jaki port musi przebywać w każdym z pośrednich stanów przy przejściu ze stanu zablokowania do stanu przekazywania ramek.

Oprócz komunikatu BPDU, mosty korzystają z jeszcze jednego typu komunikatu. Jest to powiadomienie o zmianie topologii. Format tego komunikatu pokazany jest na rysunku 9.21.



Rys. 9.21. Format komunikatu o zmianie topologii

Poszczególne pola komunikatu o zmianie topologii to:

- Identyfikator protokołu: stała równa 0.
- Wersja: stała równa 0
- Typ komunikatu: stała równa 128

#### 9.3.2.4.4 Problemy związane ze stosowaniem mostów przeźroczystych

Łączenie sieci LAN za pośrednictwem mostów przeźroczystych stwarza kilka problemów dotyczących jakości transmisji, wśród których najistotniejsze to:

- **Wzrost prawdopodobieństwa utraty ramek**, w wyniku usuwania ramek, związanego z przeciążeniem sieci, do której mają być one przesłane przez most,
- **Wzrost opóźnienia**, związany z oczekiwaniem ramek na obsługę w moście i czasem samej obsługi (filtracji).

- Wzrost "czasu życia" ramki spowodowany wzrostem opóźnienia.
- Zwiększenie stopy błędów, wynikające z każdorazowego obliczania nowej cyklicznej sumy kontrolnej podczas zmiany formatu ramki (w przypadku łączenia różnych typów sieci LAN). Ponieważ standard nie wymaga, aby suma kontrolna pozostawała niezmieniona (nawet wtedy, gdy jest to możliwe, tzn. gdy łączone są sieci tego samego typu), niektóre mosty przeźroczyste mogą ją zmienić nawet w przypadku łączenia sieci tego samego typu.
- Zmiana kolejności ramek - możliwa podczas aktualizacji drzewa opinającego.
- Wzrost prawdopodobieństwa generacji kopii ramek, wynikający z możliwości powielania ramek podczas zmian w topologii drzewa opinającego.

Zastosowanie mostów, oprócz obniżenia jakości transmisji, może spowodować i inne niekorzystne zmiany w funkcjonowaniu sieci. Poniżej prezentujemy niektóre z nich.

- Sieci muszą używać ramek krótszych od maksymalnego dopuszczalnego rozmiaru ramki.

W połączonych mostami sieciach, z różnymi maksymalnymi rozmiarami ramek, pojawienie się ramki o zbyt dużym rozmiarze spowoduje jej odrzucenie.

Rozwiązaniem może być ograniczenie maksymalnej długości ramek, przez wybór najmniejszego z maksymalnych rozmiarów dopuszczalnych w poszczególnych sieciach. Zapobiega to co prawda utracie zbyt długich ramek, ale zmniejsza wykorzystanie przepustowości sieci.

Inną metodą może być fragmentacja i składanie ramek przez urządzenia sprzągające sieci. Wymaga to jednakże łączenia sieci na poziomie warstwy sieciowej.

Skuteczne rozwiązywanie tego problemu zapewnia sterowanie źródłowe (ang. *source routing*); stacje końcowe same negocjują wówczas maksymalny rozmiar przesyłanych ramek.

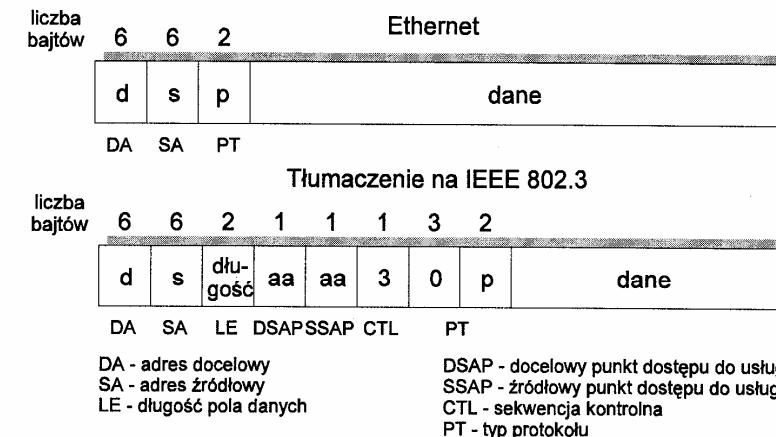
- Informacje specyficzne dla danego typu sieci mogą zostać stracone.

Informacjami specyficznymi dla danego typu sieci są priorytety ramek. Przykładowo, ramka może być transmitowana z sieci źródłowej, nadającej priorytety, poprzez sieć „tranzytową”, która ich nie uwzględnia, do sieci docelowej uwzględniającej priorytety. W takim przypadku, nie ma możliwości odtworzenia poczatkowej wartości priorytetu.

- Możliwa jest nieprzewidziana zmiana formatu ramki

Formaty ramek sieci Ethernet i ramek zgodnych ze standardem IEEE 802.3 różnią się nieco. Ramka IEEE 802.3 zamiast pola typu ramki, używanego w Etherencie, zawiera pole długości danych, a pole danych zawiera dodatkowo informacje dotyczące podwarstwy kanału logicznego.

## 9.3.2 Mosty



Rys. 9.22. Ramka sieci Ethernet i jej tłumaczenie na standard IEEE 802.3

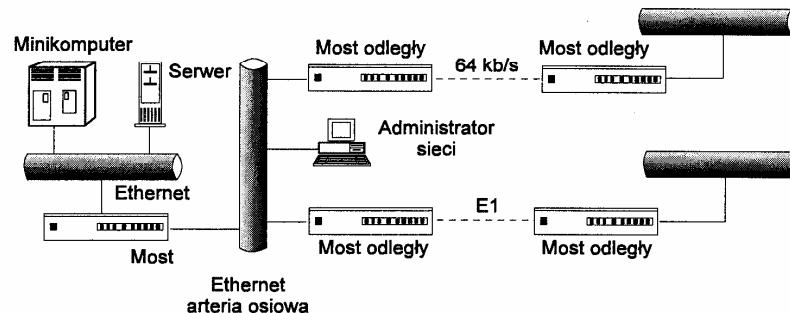
Propozycja RFC 1042 opisuje format ramki IEEE 802.3 odpowiadający formacie sieci Ethernet (patrz rysunek 9.22). Pierwsze trzy bajty pola określającego typ protokołu są równe zero, a kolejne dwa stanowią przekopiowane z ramki Ethernet 2-bajtowe pole typu ramki. Ramka Ethernetu przetłumaczona na format IEEE 802.3 może być poddana łatwiejszej konwersji na inne formaty odpowiadające standardom IEEE 802.X sieci LAN. Kłopot pojawi się w chwili, gdy ramka ma być ponownie przesłana do sieci Ethernet. Na podstawie pola typu, w którym trzy pierwsze bajty są równe zero, most nie może określić, czy ramka została wysłana z sieci Ethernet, czy też z sieci LAN IEEE 802.3. Analogicznie, ramka wysłana w formacie IEEE 802.3 może zostać odebrana w formacie Ethernet. Taka zmiana formatu ramki może uniemożliwić prawidłową pracę niektórych protokołów. Produkowane obecnie mosty potrafią jednakże rozpoznawać format początkowy ramki (Ethernet względnie IEEE 802.3).

## 9.3.2.4.5 Most odległy

Szczególnym typem mostu przeźroczystego jest most odległy (ang. *remote bridge*) nazywany również mostem dystansowym oraz półmostem (ang. *half bridge*). Służy on do łączenia odległych od siebie sieci lokalnych. Most jest przyłączany do każdej z sieci, a następnie oba mosty są łączone za pomocą łącznika typu punkt-punkt.

Algorytm drzewa opinającego traktuje łączne punkt-punkt jako równoważne sieci LAN i zapewnia, iż każda ramka może tam dotrzeć. Jeden z mostów staje się zatem mostem "desygnowanym" dla łącznika punkt-punkt, tj. mostem traktującym to łączne jako część drzewa opinającego, do której to części będzie przesyłać ramki. Drugi most traktuje styk z łączem jako swój port do mostu korzenia. Będzie on zatem przesyłał i odbierał ramki z łączem, traktowanego jako element drzewa opinającego.

Standard określa, że mosty odległe muszą być sprzedawane w parach, pochodzących od tego samego producenta, ponieważ protokół pomiędzy mostami odległymi nie jest objęty standardem. Zwykle, przy przesyłaniu informacji łączem pomiędzy półmostami do transmitowanych ramek dodaje się pewien nagłówek traktując samą ramkę jako „dane”. Konieczne jest przy tym przesyłanie wraz z ramką informacji o jej typie, pozwalające na możliwość łączenia różnych standardów sieci LAN.



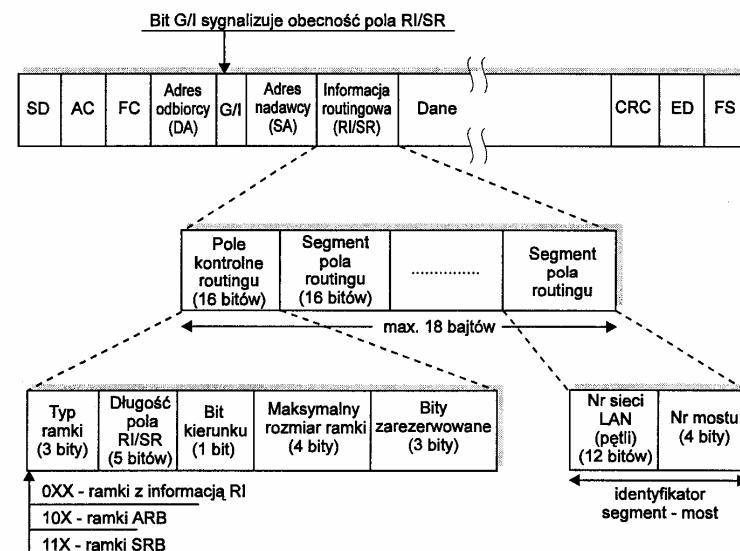
Rys. 9.23. Lokalne i odległe mosty przeźroczyste

Przykład zastosowania różnego typu mostów przeźroczystych pokazuje rysunek 9.23. Zastosowanie "lokalnych" mostów pozwala na segmentację sieci i zwiększenie jej przepustowości. Z kolei wprowadzenie mostów zdalnych umożliwia połączenie znacznie oddalonych od „centrali” sieci LAN, należących np. do oddziałów przedsiębiorstwa.

### 9.3.2.5 Source Routing

Termin „Source Routing” został wprowadzony przez firmę IBM jako nazwa mechanizmu wyznaczania optymalnej drogi między dwiema stacjami dołączonymi do połączonych sieci typu Token-Ring.

Podstawą działania tego mechanizmu jest nadanie każdej pętli sieci Token Ring 12-bitowego numeru, zwanego numerem segmentu oraz przyporządkowanie każdemu z mostów numeru 4-bitowego. Do ramki Token Ring (TR) dodawane jest specjalne pole zawierające informację o trasie, wzdłuż której ramka ma być przesłana. Obecność tego pola w ramce, zwanego polem Source Routingu lub polem z informacją routingową (ang. *Routing Information - RI*), jest sygnalizowana ustawieniem bitu G/I w adresie nadawcy na 1. Bit ten nazywany jest też bitem RIB (ang. *Routing Information Bit*). Jeżeli wspomniany bit jest równy 0, to pole Source Routingu w ramce nie występuje, a ramki traktowane są jako transparentne. Umiejscowienie elementów Source Routingu w ramce typu Token-Ring pokazano na rysunku 9.24.



Rys. 9.24. Ramka Token Ring i znaczenie poszczególnych segmentów pola routingu (RI/SR)

Informacje o typie ramki i/lub trasie jej przesłania zawarte są w polu kontrolnym (ang. *routing control field*) oraz parach identyfikatorów segment-most. Pole kontrolne routingu składa się przy tym z trzech głównych fragmentów:

1. pola typu ramki: w IEEE 802.5 definiowane są trzy typy ramek, a mianowicie ramki kierowane zgodnie z zawartą w nich informacją routingu oraz dwa typy ramek specjalnych określanych mianem all-routes broadcast (ARB) i single route broadcast (SRB), wykorzystywanych do pozyskiwania przez stację źródłową informacji routingu;
2. pola definiującego długość informacji routingu (maksymalnie 18 bajtów) dla ramek z informacją routingu;
3. pola maksymalnego rozmiaru w danej sieci LAN ramki (516, 1500, 2052, 4472 lub 8191 bajtów).

Pole routingu może zawierać maksymalnie osiem par identyfikatorów segment-most. Mosty realizujące wskazane trasy mogą być używane do łączenia różnych typów sieci lokalnych (zwykle jednak sieci Token Ring). Ponieważ różne mogą być maksymalne rozmiary ramek w poszczególnych sieciach LAN, pole maksymalnego rozmiaru ramki (ang. *maximum frame size field*) jest używane do określenia dopuszczalnego rozmiaru ramki, który może być transportowany pomiędzy tymi sieciami.

Do konstruowania baz danych routingu stacji wykorzystywane są głównie informacje adresowe zawarte w napływających do stacji ramkach. W przypadku

braku w tablicy stacji pożąданiej informacji routingowej, może być ona pozyskana z pomocą specjalnych ramek broadcastowych, określanych mianem:

- SRB - *Single-Route Broadcast* (lub *Spanning Tree Explorer*) oraz
- ARB - *All-Routes Broadcast* (lub *All Paths Explorer*).

Aby wyznaczyć trasę prowadzącą do stacji o znanym adresie MAC, lecz nieznanej lokalizacji, stacja źródłowa wysyła ramkę typu SRB z ustawioną zerową długością pola routingu RI i maksymalnym rozmiarem ramki w połączonych sieciach LAN. Mosty źródłowe odbierają i buforują wszystkie napływające do nich ramki SRB, a następnie rozsyłają je do wszystkich dołączonych do nich segmentów sieci (z wyjątkiem segmentu/portu, z którego ramka została odebrana). Procedura ta jest powtarzana przez wszystkie mosty, a kopie ramek rozsyłane są po całej sieci LAN, tak że w końcu docierają do stacji przeznaczenia, bez względu na jej położenie w sieci. Ramki SRB przesyłane są przy tym wzduż tras tworzących drzewo opinające.

Stacja docelowa, po odbiorze ramki SRB odpowiada na nią ramką typu ARB. Ramka ta nie musi być przy tym przesyłana wzduż gałęzi drzewa. Każdy most, pośredniczący w przekazie ramki ARB, po jej odbiorze, dołącza do pola routingu RI tej ramki wartość identyfikatora, tj. numeru przebytego przez ramkę segmentu i swój numer mostu, zwiększając tym samym długość informacji routingowej. Jednocześnie mosty analizują i ewentualnie modyfikują zawarty w ramce maksymalny rozmiar ramki, tj. pozostawiają go bez zmiany lub zmniejszają, do obowiązującego w danym segmencie LAN. Kopie ramek przesyłane są przez wszystkie pozostałe porty mostu. W ten sposób kopie ramki ze stacji docelowej dotrą do stacji źródłowej wszystkimi możliwymi trasami. Na podstawie ramek ARB, napływających do stacji źródłowej, stacja ta, porównując identyfikatory segmentów i mostów, dokonuje wyboru trasy najlepszej dla przekazu danych. Może nią być trasa zawarta w najwcześniejjszej ramce odpowiedzi, bądź też trasa z najmniejszą liczbą mostów i segmentów pośrednich. Wybrana trasa zostaje też umieszczona w tablicy routingu stacji i używana podczas transmisji ramek informacyjnych do danej stacji docelowej.

Ponieważ ramki ARB nie są „zmuszane” do poruszania się zgodnie z topologią drzewa opinającego, muszą być podjęte dodatkowe środki, by ramki nie krążyły w pętlach. Zanim kopia ramki typu ARB zostanie przesłana dalej, każdy most sprawdza informacje o trasie zawarte w ramce. Jeżeli sekwencja identyfikatorów segmentu wejściowego i wyjściowego wystąpiła już wraz z własnym identyfikatorem danego mostu, to ramka jest usuwana. Pojawienie się tej sekwencji oznacza bowiem, iż ramka była już wcześniej transmitowana przez ten most.

Należy zwrócić uwagę na to, że droga do stacji docelowej nie musi być szukana za każdym razem od nowa. Wystarczy raz ją znaleźć, a następnie jedynie odczytywać z tablicy tras. Ponieważ większość stacji przesyła ramki do określonej liczby stacji docelowych, liczba ramek służących do znajdowania tras jest relatywnie mała, w porównaniu z liczbą ramek informacyjnych.

Source Routing postrzegany był na początku jako elegancki i efektywny mechanizm przesyłania informacji. Wraz z wprowadzeniem mostów wieloportowych (pierwsze rozwiązania firmy IBM miały tylko dwa porty) i stosowaniem zabezpieczeń w postaci dwóch mostów podłączonych równolegle do jednego segmentu okazało się, iż ramki protokolarnie (ramki ABR) powodują duże uszczuplenie pasma sieci (w sieci z ośmioma równoległymi segmentami jedna ramka protokolarna może zostać powielona w 1000 kopii). Inną poważną wadą Source Routingu jest brak dynamicznej rekonfiguracji sieci po „upadku” łączna. Ponieważ optymalna ścieżka jest wyznaczana w fazie inicjowania sesji, zmiana trasy wymaga powtórnego nawiązania sesji.

W odróżnieniu od mostu transparentnego, most source routingowy nie tworzy żadnej tablicy adresowej. Decyzja o przesłaniu ramki na określony port podejmowana jest tylko i wyłącznie na podstawie informacji routingowej niesionej przez ramkę.

### 9.3.2.6 Porównanie mostów przeźroczystych i źródłowych

Podstawowe różnice pomiędzy poszczególnymi rodzajami mostów, jak i wynikające z nich wnioski, można sformułować następująco:

- W sieciach wykorzystujących mosty przeźroczyste, decyzje dotyczące wyboru trasy przesyłania ramek podejmowane są przez same mosty. Może to mieć istotny i niekorzystny wpływ na działanie sieci, w przypadku sieci bardzo dużych. Czas przetwarzania ramek może się wówczas niebezpiecznie wydłużać.
- W sieciach wykorzystujących mosty ze źródłowym wyborem trasy, odpowiedzialność za wybór trasy spada na stacje końcowe, zwiększając tym samym ich obciążenie i wymuszając użycie procesorów o większej mocy obliczeniowej, co podraża ich koszt.
- Czas przetwarzania ramek w mostach przeźroczystych jest większy niż w mostach ze źródłowym wyborem trasy, o czas wyboru dalszej trasy przesyłania ramek.
- Okresowa wymiana ramek typu BPDU w sieciach wykorzystujących mosty przeźroczyste, pozwala na szybką reakcję mostów, w przypadku wystąpienia uszkodzeń w sieci.
- Realizacja algorytmu drzewa opinającego, powoduje blokadę niektórych portów, zmniejszając tym samym dostępną przepustowość dla segmentów sieci LAN.
- Ze względu na możliwość wystąpienia uszkodzeń w sieci, w sieciach wykorzystujących mosty ze źródłowym wyborem trasy, wymagana jest okresowa aktualizacja przechowywanych w stacjach źródłowych danych o routingu. Wiąże się to z koniecznością wysyłania co określony czas ramek rozgłoszeniowych, zwiększających obciążenie w sieci.

### 9.3.2.7 Mosty SRT

Ze względu na potrzebę łączenia sieci, w których wykorzystywane są różne algorytmy zestawiania tras, opracowano nowy rodzaj mostu - SRT (ang. *Source Routing Transparent*), pozwalający na pracę, w zależności od segmentu sieci, jako most przeźroczysty, bądź ze sterowaniem źródłowym. Mosty tego typu mają możliwości filtrowania od 20 do 30 tysięcy ramek/s.

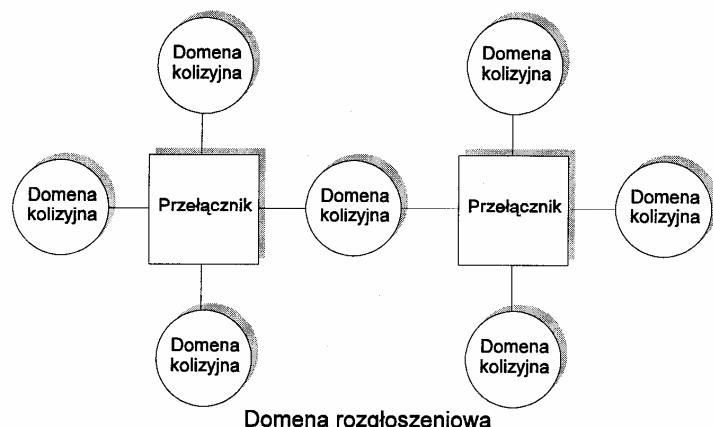
### 9.3.3 Przelączniki sieciowe i huby przelączające

W lokalnych sieciach komputerowych, wykorzystujących metody dostępu rywaliizacyjnego do wspólnego medium komunikacyjnego, podstawowe problemy ich funkcjonowania wynikają z:

- kolizji ramek w dostępie do kanału,
- występowania tzw. sztormów ramek rozgłoszeniowych.

**Przelączniki sieci LAN** (ang. *LAN Switches*) są urządzeniami wieloportowymi pozwalającymi na poprawę parametrów pracy sieci (głównie sieci Ethernet, IEEE 802.3) dzięki efektywnej segmentacji sieci na tzw. domeny kolizyjne, najczęściej bez zmian w okablowaniu i kartach sieciowych. Ponadto oferują one możliwość tworzenia wirtualnych sieci VLAN (ang. *Virtual Local Area Network*), czyli logicznego grupowania użytkowników, niezależnie od ich fizycznej lokalizacji.

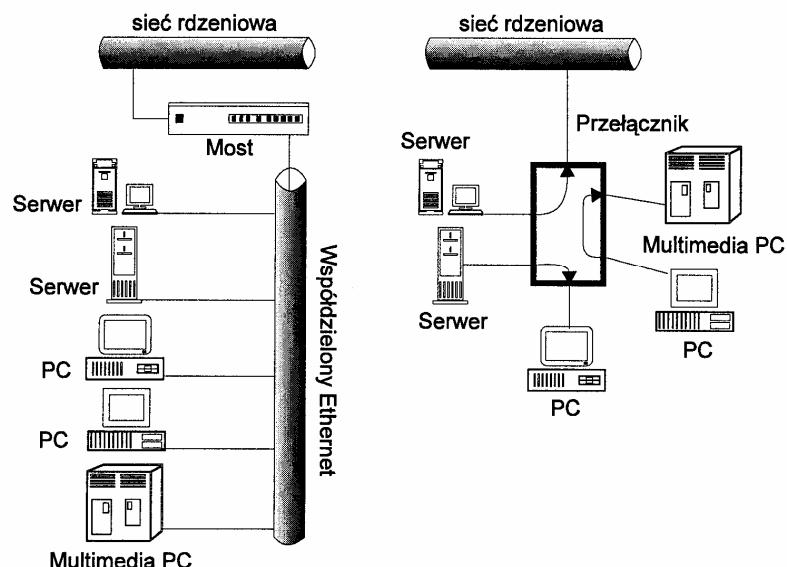
Domena kolizyjna to fragment sieci, który tworzą stacje końcowe przyłączone np. do jednego kabla czyli współdzielące medium. Z kolei obszar, na którym rozprzeszreniają się ramki rozgłoszeniowe, określany jest mianem domeny rozgłoszeniowej.



Rys. 9.25. Zastosowanie przełączników w lokalnej sieci komputerowej

Przelącznik spełnia rolę izolującą domeny kolizyjne, zwiększając jednocześnie pasmo (przepustowość) dostępne dla stacji komputerowych. Nie zapobiega on jednak rozprzeszrenianiu się wiadomości rozgłoszeniowych (patrz rysunek 9.25).

Wysłanie ramek przez jedną ze stacji z domeny kolizyjnej powoduje zajęcie medium i wstrzymanie ewentualnego wysyłania ramek przez inne stacje, należące do tej samej domeny kolizyjnej. Oczywiście w momencie wzrostu liczby stacji należących do tej samej domeny kolizyjnej, wzrasta ruch w sieci i maleje jej wydajność. Przelączniki pozwalają, w zasadzie bez przebudowy fizycznej struktury sieci, rozseparować jedną dużą domenę kolizyjną na kilka mniejszych i w ten sposób zwiększyć pasmo dostępne dla użytkowników końcowych. Zasadę działania przełącznika ilustruje rysunek 9.26.



Rys. 9.26. Różnica w działaniu pomiędzy mostem a przełącznikiem

Przelączniki pracują bardzo szybko, dzięki wyposażeniu ich w szybkie szyny danych i specjalizowane układy obsługujące ruch ramek. Są to więc urządzenia korzystające głównie z rozwiązań sprzętowych. Z tego względu stosuje się je tam, gdzie trzeba zapewnić dedykowane pasmo dla specyficznych użytkowników lub dla grup roboczych z własnymi serwerami, pracujących w technologiach: Ethernet, Token Ring, FDDI, szybki Ethernet i ATM.

Generalnie przełącznik operuje na poziomie warstwy drugiej i jest urządzeniem funkcjonalnie bardzo zbliżonym do mostu. Podejmuje on decyzje o przesłaniu

ramki na podstawie adresu docelowego MAC i informacji zawartej w tablicy adresowej. Maksymalna wielkość tablicy adresowej jest przy tym parametrem charakterystycznym każdego przełącznika i limituje liczbę stacji roboczych podłączonych do niego. Są też przełączniki, które oprócz ograniczonej, globalnej liczby adresów, mają limitowaną liczbę adresów dla poszczególnych portów. Jedną z różnic pomiędzy przełącznikiem a mostem jest posiadanie kilkunastu lub kilkudziesięciu portów wejścia/wyjścia w przypadku przełącznika i zwykle dwóch (kilku) portów w przypadku mostu.

W chwili obecnej przełączniki zdecydowanie wypierają tradycyjne mosty, a ciągłe rozszerzanie zakresu realizowanych przez nie funkcji wpływa również na coraz częstsze ich instalowanie w miejsce routerów.

### 9.3.3.1 Różnice pomiędzy mostem i przełącznikiem

**Funkcjonalnie przełączniki sieci LAN pełnią zadania mostów, sprzągając poszczególne urządzenia sieci lokalnej.** Technologie budowy sieci w oparciu o mosty pozwalają odseparować od siebie poszczególne grupy robocze, ale w dalszym ciągu nie pozwalają uwolnić się od wspólnego segmentu sieci (sieci szkieletowej) łączącego kolejne mosty. W momencie znacznego wzrostu liczby dołączonych do sieci LAN stacji końcowych rodzi się problem bądź zainstalowania kolejnego mostu, bądź też coraz większego niekorzystnego obciążania jednego z segmentów sieci. W przypadku przełącznika, posunięciem analogicznym do zakupu kolejnego mostu jest wykorzystanie kolejnego portu w przełączniku. Podstawowa różnica pomiędzy mostem, a przełącznikiem została przedstawiona na rysunku 9.26. Rysunek ten ilustruje sposób podłączenia mostu i przełącznika do sieci LAN. Most nie ingeruje w pracę wewnętrz danej podsieci komputerowej, lecz spełnia rolę izolującą ruch ramek pomiędzy podsieciami, zwiększać w ten sposób wydajność każdego z rozdzielonych segmentów sieci LAN. W przypadku przełącznika mamy często do czynienia z sytuacją odmienną: do jego portów przyłączane są stacje komputerowe (rzadziej podsieci), dzięki czemu komutuje on ramki tylko pomiędzy tymi stacjami (bądź sieciami), do których adresowane są dane. Komutacja (przełączanie) odbywa się na podstawie adresów podwarstwy MAC, z dynamicznym ich wykrywaniem w czasie pracy sieci LAN. Porównanie mostów i przełączników zawiera tabela 9.2.

Tabela 9.2. Porównanie mostów i przełączników

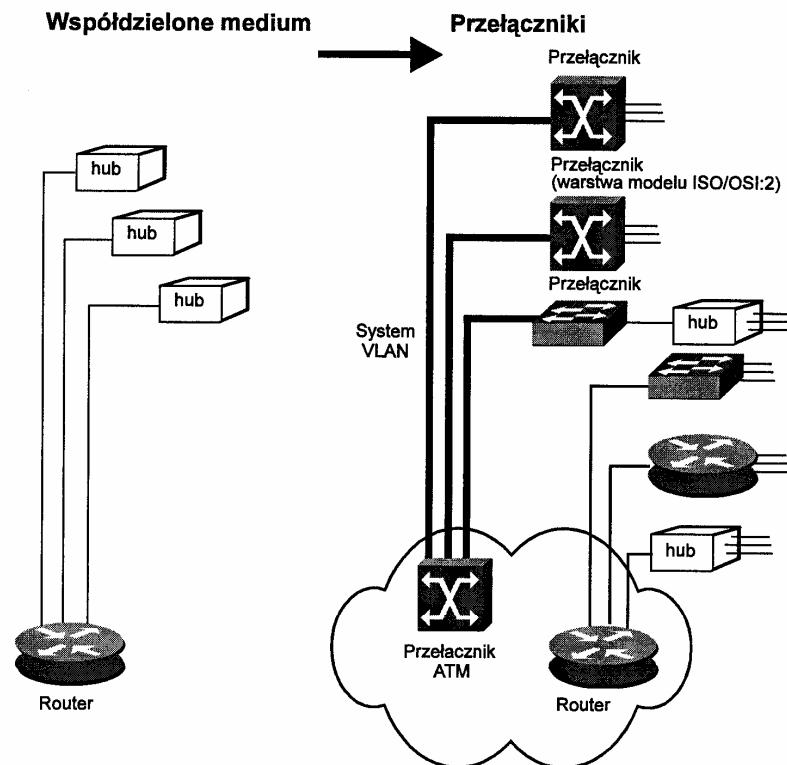
Most	Przełącznik
Operuje na poziomie podwarstwy MAC; algorytm buforowania i przesyłania ramek analizuje całą ramkę, zanim zostanie ona przesłana dalej, (store-and-forward)	Operuje na poziomie podwarstwy MAC, z możliwością wspierania ruchu pakietów warstwy sieciowej; algorytm buforowania i przesyłania ramek analizuje bądź całą ramkę, zanim zostanie ona przesłana dalej, (store-and-forward), bądź tylko jej część (cut through, fragment-free)

Tabela 9.2. Porównanie mostów i przełączników (c.d.)

Most	Przełącznik
Nie realizuje skomplikowanych protokołów wyboru trasy; nie zapewnia transferu wieloma trasami jednocześnie, w razie zerwania połączenia w sieci; konieczna jest rekonfiguracja topologii logicznej sieci	Niektoře mogą realizować jedynie protokół drzewa opinającego, przełącznik nie realizuje połączeń wieloma trasami jednocześnie, ale daje możliwość skonfigurowania łącz zapasowych
Łączy bądź rozdziela ruch pomiędzy segmentami sieci lokalnych lub metropolitarnych	Realizuje połączenia pomiędzy pojedynczymi urządzeniami w sieci, bądź pomiędzy segmentami sieci lokalnych z możliwością tworzenia wirtualnych grup (VLAN)
Pozwala łączyć sieci lokalne i metropolitarne znajdujące się zarówno w niewielkich jak i dużych odległościach od siebie	Pozwala łączyć sieci lokalne znajdujące się blisko siebie
(Zwykłe) jednolita przestrzeń adresowa oparta na adresach podwarstwy MAC	Tablice adresów są zwykle jednolite, zawierają adresy stacji, bądź porty przynależące do danej sieci wirtualnej
Liczba adresów proporcjonalna tylko do liczby urządzeń w sieci; most obsługuje od kilkuset do kilkunastu tysięcy adresów podwarstwy MAC	Liczba adresów proporcjonalna do urządzeń w sieci, bądź liczby portów z możliwością przełączania; obsługuje od kilku do kilkunastu tysięcy adresów podwarstwy MAC
Slabe mechanizmy ochronne; przeżroczy dla protokołów wyższych warstw, transportuje wiadomości rozgłoszeniowe wyższych warstw pomiędzy segmentami sieci	Mogość zapewnienia wysokiego poziomu bezpieczeństwa, z filtracją inteligentną, tzn. pozwalającą filtrować nawet usługi warstwy aplikacji (sprawdzanie pól w każdej ramce)
Nie zapewnia bezpieczeństwa w sieci, a jedynie kontrolę ruchu pomiędzy segmentami sieci	Zapewnia bezpieczeństwo na poziomie adresów podwarstwy MAC, z możliwością ścisłego określenia ruchu pomiędzy stacjami komputerowymi bądź innymi urządzeniami w sieci (VLAN)
Tani	W zależności od konfiguracji: tani lub średnio drogi
Prosty w instalacji, konfiguracji i obsłudze	Bardzo prosty w instalacji, wymagający konfiguracji tylko w przypadku tworzenia wirtualnych sieci, co również nie jest trudne

**Przełącznik likwiduje podstawowe ograniczenie, wynikające z metody dostępu do medium komunikacyjnego, którym jest opóźnienie w przekazie ramek. Przełącznik retransmituje ramki prawie natychmiast, co najwyższej buforując je w porcie, do którego przyłączona jest stacja docelowa (lub źródłowa).**

Rysunek 9.27 ilustruje ewolucję urządzeń sprzągających, stosowanych w lokalnych sieciach komputerowych.



Rys. 9.27. Ewolucja lokalnych sieci komputerowych w kierunku przełączania

### 9.3.3.2 Routery a przełączniki

Jak wspomniano powyżej, **przełączniki pozwalają „zwiększać” przepustowość sieci poprzez segmentację jednej dużej, „zatłoczonej” domeny kolizyjnej na kilka mniejszych. Każda nowa „poddomena” dysponuje pojedynczym portem przełącznika.** Idealna sytuacja ma miejsce, gdy pojedynczy port w przełączniku jest połączony z jedną stacją roboczą; domenę kolizyjną stanowi wtedy pojedynczy komputer. Tym samym wyeliminowane zostają jakiekolwiek kolizje ramek. Pasmo gwarantowane przez port, do którego przyłączony jest komputer, staje się pasmem dedykowanym dla konkretnej stacji. Oczywiście, w momencie gdy liczba stacji przyłączonych do jednego portu rośnie, rośnie też i liczba kolizji pociągając za sobą zwykłe konieczność podziału domeny. Przełączniki w prosty sposób pozwalają sterować ruchem ramek w obrębie domen kolizyjnych, jednak ich „zdolności” kończą się na poziomie domen rozgłoszeniowych. Ramki rozgłoszeniowe są przesyłane po

wszystkich portach, oprócz portu, z którego zostały odebrane, i z tego powodu mogą stanowić zagrożenie dla prawidłowej pracy sieci, prowadząc do przeciążenia. Aby odseparować od siebie dwie domeny rozgłoszeniowe nieodzowny jest router, operujący w trzeciej warstwie. Przełączniki są urządzeniami bardzo szybkimi i w związku z tym nie utrzymującymi złożonych tablic routingu. Z kolei routery pracują znacznie wolniej, lecz ich działanie jest „efektywniejsze”. Wynika to z faktu, że oprócz podziału sieci na domeny kolizyjne dzielą również sieć na domeny rozgłoszeniowe. Stosowanie routerów wszędzie tam, gdzie dochodzi do zatłoczenia sieci, byłoby nieracjonalne i rozrzutne. Rozwiązań najkorzystniejszym wydaje się być komplementarne stosowanie routerów i przełączników: routerów do separacji grup oddziałowych (domen rozgłoszeniowych), w oparciu o podział na podsieci na poziomie adresów IP, oraz przełączników do tworzenia grup roboczych w ramach sieci oddziałowych (patrz rysunek 9.27).

### 9.3.3.3 Tryby pracy przełączników i metody przełączania

Technologia przełączania w sieciach LAN pojawiła się stosunkowo niedawno, ale zdążyła już stać się dojrzałą i obiecującą metodą łączenia sieci. Ogólnie, **przełącznik jest urządzeniem zdolnym do równoczesnej transmisji ramek pomiędzy kilkoma parami portów**. Jest to cecha wspólna urządzeń tej klasy. Techniki podejmowania decyzji o transmisji i sposoby rozpoznawania struktury sieci są różne w różnych produktach producentów, stanowiąc podstawę klasyfikacji przełączników sieci LAN.

Do metody rozpoznawania struktury sieci, tzn. ustalania do jakich portów przełącznika podłączone są poszczególne sieci, wszystkie oferowane urządzenia wykorzystują ten sam mechanizm analizy adresu nadawcy w ramce i tworzenia, w oparciu o tę informację, „tablic przełączania” - jednoznacznie kojarzącą adres źródłowy (MAC) stacji z numerem portu, do którego stacja jest przyłączona. Wszystkie przełączniki utrzymują tablice adresowe, a ich rozmiar jest jednym z parametrów określających możliwości przełącznika, jeśli chodzi o maksymalną liczbę stacji do niego przyłączonych.

Współczesne przełączniki realizują dwa podstawowe tryby pracy: przełączania przeźroczystego (ang. *Transparent Bridging* - TP) lub przełączania szybkiego bądź ekspresowego (ang. *Express Switching* - ES).

Pierwsza z metod jest w zasadzie przewidziana do pracy w sieci z pojedynczym przełącznikiem i nie umożliwia skonfigurowania wyróżnionego portu do komunikacji z innym przełącznikiem. Wszystkie porty traktowane są jako równorzędne. Ramki o znanym adresie kierowane są do odpowiedniego portu, a o nieznanym adresie rozsypane są do wszystkich portów. Przełącznik taki potrafi przesyłać ramki „do wszystkich” i „do wielu”.

Druga metoda - szybkiego przełączania - pozwala na wyodrębnienie pojedynczego portu służącego do połączenia z innymi przełącznikami, tzw. portu backbone lub portu do „reszty świata”. Jest to bardzo cenna cecha pozwalająca na stop-

nową rozbudowę sieci oddziałowej, przy zachowaniu niezmienionej przepustowości dla stacji już będących w sieci. Podstawowa zasada przełączania w przełączniku pracującym w tym trybie jest następująca: ramki o znany adresie przełączane są na odpowiedni port, ramki o nieznany adresie przełączane są na port backbone. Przełącznik „uczy się” adresu w momencie odbioru pierwszej ramki z portu „wewnętrznego” sieci, jednak nie uczy się adresów zawartych w ramkach pochodzących z portu backbone. Taka konstrukcja algorytmu przełączania ramek jest bardzo efektywna (chociażby ze względu na możliwość dołączania nowych przełączników), jednak niesie za sobą pewne niebezpieczeństwo utraty ramek na początku działania sieci. Wiąże się ono z wysłaniem „w świat” ramki zaadresowanej do stacji lokalnej, której adresu przełącznik nie zdążył się jeszcze nauczyć (stacja nie wysłała jeszcze żadnej ramki). Wszystkie przełączniki bez względu na to, czy pracują w oparciu o metodę TB czy ES, nie wysyłają ramki do portu, z którego ramka napłynęła.

**Procesy przełączania** mogą być realizowane zgodnie z jedną z czterech podstawowych metod:

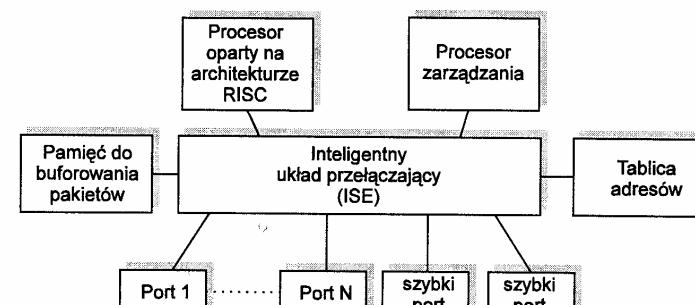
1. **Skróconej analizy adresu** (ang. *Cut-Through (C-T)*). Zgodnie z tą metodą przełącznik czyta i analizuje jedynie początek ramki z adresem docelowym i podejmuje natychmiastową decyzję o wyborze portu. Metoda ta gwarantuje minimalne opóźnienia (ok. 40 mikrosekund) w skierowaniu pierwszego bitu ramki na port przeznaczenia. Wadą tej metody jest możliwość przesyłania do innych domen (stacji) ramek biorących udział w kolizji. Informacja o interferencji ramek może bowiem dotrzeć do przełącznika z opóźnieniem nieco większym. Inną wadą metody C-T jest też zagrożenie związane z przesyłaniem ramek z błędymi sumami kontrolnymi.
2. **Analizy minimalnej długości ramki** (ang. *Fragment-Free (F-F)*). W tym przypadku przełącznik czeka ze skierowaniem ramki do portu docelowego do chwili odebrania i przeanalizowania pierwszych 64 bajtów ramki, tak, by zgodnie ze standardem Ethernet, wyeliminować ewentualną transmisję ramek zniekształconych na skutek kolizji. Metoda F-F wprowadza dodatkowe opóźnienie „w przełączaniu” ramki o około 65 mikrosekund.
3. **Komutacji ramek** (ang. *Store-and-Forward (S-F)*). W metodzie tej konieczny jest odbiór całej ramki. Skierowanie ramki do portu docelowego może mieć miejsce wtedy i tylko wtedy, gdy nie zostanie wykryty błąd. W tym przypadku opóźnienia w przełączaniu uzależnione są od długości przesyłanych ramek. Dla ramek krótkich czasy te są porównywalne z otrzymanymi dla metody F-F. Z kolei w przypadku ramek długich, 1518-bajtowych, czas ten rośnie do 1.2 milisekundy. Metoda ta ma szereg zalet. Najważniejsze spośród nich to:
  - błędne pakiety są wychwytywane i nie ulegają dalszej propagacji;

- przy odpowiednio dużych wielkościach buforów w portach, nie występuje problem z przesyłaniem ramek pomiędzy portami o różnych przepustowościach;
- może następować konwersja danych na poziomie warstwy MAC, przy czym konwersja taka wymaga pełnego buforowania danych (przełącznik realizuje wówczas funkcje mostu tłumaczącego (ang. *translating bridge*)).

4. **Przełączania inteligentnego** (ang. *Intelligent Switching (I-S)*). Metoda ta łączy w sobie algorytmy pracy C-T i S-F, w ten sposób, że przy małym ruchu i niskim prawdopodobieństwie błędów praca przełącznika przebiega w trybie C-T. Gdy liczba błędów rośnie, następuje automatyczne przełączenie trybu pracy na S-F.

#### 9.3.3.4 Architektura przełącznika

Architektura przełącznika, z podaniem jego najważniejszych bloków funkcyjnych, została przedstawiona na rysunku 9.28.



Rys. 9.28. Architektura przełącznika

Podstawowym elementem przełącznika jest wysoce specjalizowany układ scalony nazywany często przez producentów ISE (ang. *Intelligent Switch Engine*) czyli układ scalony typu ASIC (ang. *Application Specific Integrated Circuit*). Zadaniem tego układu jest przełączanie i filtracja ramek, zgodnie z instrukcjami otrzymywanymi z centralnego procesora. Możliwości komutacyjne wytworzonych obecnie układów scalonych pozwalają zwykle na obsługę od 500000 - 600000 ramek na sekundę (ramek 64 bajtowych). Z kolei wydajność przełącznika w zakresie filtracji sięga 1 200 000 ramek/s. Przydziela pamięci przeznaczoną do przechowywania ramek, które nie mogą być obsłużone w danej chwili, może być, w zależności od producenta, dynamiczny lub statyczny. Bufor statyczny ma zgodnie z jego nazwą stałą pojemność i jest przypisany do danego portu. Jego wielkość jest rzędu 128 kB - 256 kB, dla portów wolniejszych (10 Mb/s, 16 Mb/s) i 512 kB - 1 MB dla por-

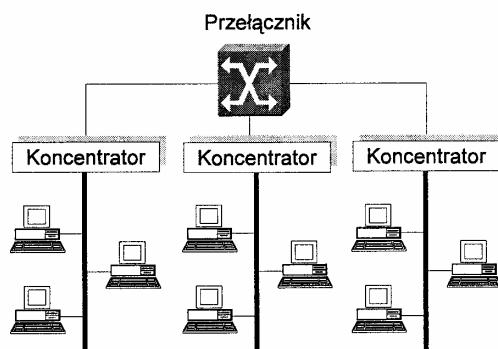
tów obsługujących sieci FDDI, ATM, Fast Ethernet czy 100VG-AnyLAN. Bufory dynamiczne różnią się od statycznych tym, iż oprócz pamięci przydzielonej danemu portowi dysponują pamięcią wspólną, z możliwością jej wykorzystania przez te porty, które w danej chwili mają zwiększoną liczbę ramek do obsłużenia. Pamięć ta jest dynamicznie alokowana dla danego portu. W tym przypadku wielkość pojemności bufora przypadająca na dany port może być mniejsza, np. rzędu 64 kB dla portów 10Mb/s i 16 Mb/s oraz 512 kB dla portów szybkich. Z kolei wielkość pamięci współdzielonej jest rzędu 2 MB - 4 MB.

### 9.3.3.5 Praktyczne zastosowanie przełączników

Przełączniki, stające się coraz bardziej popularnymi elementami sieci lokalnych, mogą przejmować funkcje lokalnej arterii osiowej, zwiększać efektywność pracy grup roboczych oraz realizować podział logiczny sieci na segmenty.

#### Stosowanie przełączników i arterii osiowych

Użycie przełącznika jako arterii osiowej (w punkcie centralnym sieci - PCS) zwiększa wielokrotnie pasmo transmisyjne całej arterii. Każda niezależna sieć lokalna jest połączona z przełącznikiem za pośrednictwem koncentratorów (hubów), przy czym szybkości przełączania (obsługi ramek) przełącznika i koncentratorów są zbliżone. Architektura taka (patrz rysunek 9.29) pozwala na lokalizację serwerów, zwykle rozproszonych, w jednym centralnym miejscu. Ułatwia ona również zarządzanie siecią i poprawia jej fizyczne bezpieczeństwo. W efekcie zarządzanie siecią wymaga mniej czasu (i ludzi), co obniża koszt tej operacji, a dostępne pasmo przełącznika (np. 1.28 Gb/s) umożliwia łączenie ze sobą setek lub tysięcy użytkowników sieci LAN.



Rys. 9.29. Przełączana arteria osiowa

Opisane rozwiązanie nie zawsze jest możliwe do zastosowania. W sytuacji, gdy poszczególne jednostki organizacyjne używają swoich własnych sieci i są położone

w znacznie oddalonych od siebie miejscach, nieodzowne staje się wykorzystanie "tradycyjnej" arterii osiowej opartej na sieci lokalnej lub miejskiej (np. FDDI). Przełącznik oferuje, w porównaniu z arterią osiową, kilka alternatywnych rozwiązań w postaci współdzielonej sieci LAN lub MAN:

#### Przelaczanie pomiędzy sieciami Ethernet i FDDI

Pierścień FDDI zapewnia szybkie i bezpieczne połączenia na dużych odległościach pomiędzy różnymi koncentratorami. Użytkownicy korzystają z takich udogodnień, jak tworzenie sieci wirtualnych, nadawanie priorytetów pakietom i zarządzanie minimalizujące możliwość kolizji.

#### Przelaczanie pomiędzy sieciami FDDI

Dwie sieci FDDI są łączone za pomocą szybkiej magistrali, gwarantując zalety obu szybkich technologii.

#### Przelaczanie pomiędzy FDDI i grupą serwerów

Konfiguracja korzystna dla sieci, które używają FDDI, jako alternatywnego środka komunikacji likwidującego "wąskie gardło". Rozwiązanie to jest zalecane dla dużych sieci typu klient-serwer. Może być ono również używane, gdy grupa serwerów jest bezpośrednio połączona ze współdzielonym pierścieniem FDDI.

#### Routowane połączenie z FDDI

Wielu użytkowników potrzebuje połączenia pomiędzy siecią lokalną z przełącznikiem i arterią FDDI. Łącząc dodatkowo porty przełącznika z routera, sprzągającymi segmenty sieci, otrzymujemy szybkie połączenie z FDDI wraz z możliwościami wyboru tras, dostarczonymi przez router. Każdy port obsługuje inną grupę użytkowników (sieć wirtualna).

#### Arteria osiowa utworzona z przełączników

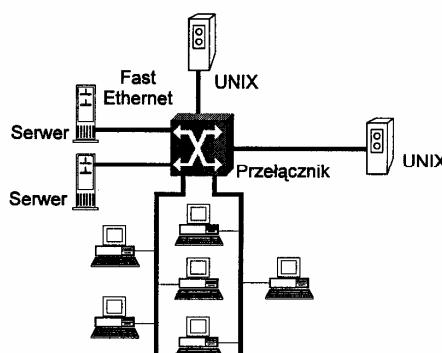
Arteria taka może zostać utworzona poprzez połączenie przełączników światłowodami. Jest użyteczna do tworzenia szybkiego łącza pomiędzy użytkownikami połączonymi metodą szybkiego przełączania portów.

#### Przełączniki w sieciach typu klient-serwer

Dynamiczne przełączanie portów jest korzystne, kiedy stacja klienta i serwer wykazują dużą wrażliwość na parametry pasma transmisyjnego oraz wymagają oddzielnego kanału transmisyjnego. Przełączanie dynamiczne zapobiega wówczas opóźnieniom, które są niepożądane dla aplikacji zależnych od czasu (np. video-konferencje). Słabym punktem mogą stać się jednak serwery, dla których pasmo jest ograniczone. Rozwiązaniem może być szybki Ethernet, który zapewnia szybkość transmisji 100 Mb/s w połączeniu z serwerami.

Ważnym zagadnieniem, łączącym się z funkcjonowaniem sieci klient-serwer jest wadliwa organizacja interfejsu do serwera (zasobów współdzielonych) i potencjalne "wąskie gardło", powstające gdy wielu użytkowników chce równocześnie uzyskać dostęp do współdzielonych urządzeń. Oprócz alokacji kanałów dedykowanych dla każdego serwera, można zwiększyć pasmo transmisyjne przy użyciu przełącznika, instalując w serwerach po kilka interfejsów i łącząc je z przełącznikiem za pośrednictwem dynamicznie przełączanych portów. Jest to niedroga metoda dzielenia sieci lokalnej na mniejsze segmenty, zapewniająca komunikację międzysieciową w postaci logicznego łącza realizowanego przez oprogramowanie serwera.

Zależnie od środowiska i typu serwera interfejsy mogą być także przypisywane różnym sieciom wirtualnym. Przypisanie jednego interfejsu do danej sieci wirtualnej oddziela i chroni ruch pomiędzy różnymi interfejsami danego serwera. Przykładowe środowisko klient-serwer pokazuje rysunek 9.30.



Rys. 9.30. Środowisko klient-serwer z dynamicznym przełączaniem portów

#### Podział logiczny sieci na segmenty

Logiczna segmentacja sieci prowadzi do poszerzenia dostępnego pasma transmisyjnego, zapewniając tym samym grupom użytkowników lepsze możliwości komunikacyjne. Topologia gwiazdy, z centralnym przełącznikiem, eliminuje nadmiarowość informacji „protokolarnej” wymienianej w sieciach współdzielonych oraz ogranicza koszty związane z tłumaczeniem protokołów. Topologia tego typu zmniejsza też koszt instalacji i obsługi sieci oraz zwiększa efektywną zaagregowaną przepustowość sieci.

Logiczna segmentacja oferuje dwie podstawowe zalety, w porównaniu z fizycznym dzieleniem sieci przy użyciu routera:

- **Łatwość realokacji stacji w sieci** - jeśli sieć jest dzielona na podsieci przy pomocy routera, realokacja stacji wymaga fizycznego przemiesz-

czenia urządzenia i rekonfiguracji routera. Użycie przełącznika zapewnia programową realokację urządzenia.

- **Szybkości pracy** - użycie routera pomiędzy segmentami powoduje nadmiarowość przesyłania i przetwarzania informacji oraz redukuje wydajność całego systemu. Każdy pakiet przesyłany pomiędzy segmentami lub segmentem i routерem jest opóźniany na skutek dokonywanej w routerze analizy. Przełączanie nie powoduje nadmiarowości i umożliwia transport pakietów pomiędzy segmentami oraz segmentami i serwerami z szybkością równą szybkości medium transmisyjnego.

#### Podsumowanie zastosowań przełączników

Można wyróżnić trzy podstawowe zastosowania przełączników:

- **Integrowanie elementów systemu rozprozonego** - najczęściej w Punkcie Centralnym Sieci (PCS), w którym zbiegają się połączenia pochodzące od wszystkich jej segmentów.
- **Zapewnianie szybkich połączeń** z arterią osiową bądź siecią szkieletową (ang. *campus backbone*) i serwerami. Uzyskuje się to przez zastosowanie w PCS inteligentnych hubów przełączających.
- **Skalowanie pasma sieci** przez wykorzystanie coraz większej liczby portów przełączników, co jest równoznaczne z segmentacją sieci. Segmentacja może się odbywać w przełącznikach zainstalowanych w PCS i/lub grupach roboczych.

Wymienione zastosowania są realizowane przez przełączniki pracujące w centralnym punkcie sieci lub w grupie roboczej. Każde z tych rozwiązań charakteryzuje się przy tym zespołem ważnych cech:

#### Przełącznik w centralnym punkcie sieci

Nowoczesne sieci zakładowe posiadają centralny punkt sieci (PCS), z którego steruje się sieciami wirtualnymi, segmentacją i zarządzaniem całą siecią zakładową. W PCS znajduje się przełącznik zwany inteligentnym hubem przełączającym, który musi spełniać szereg wymagań:

- wysoki poziom niezawodności,
- maksymalnie szerokie pasmo agregowanych sieci,
- modułarna konstrukcja zapewniająca integrowanie sieci LAN o zróżnicowanych technologiach i wymiarach,
- współpraca z szybką magistralą (FDDI, ATM, Fast Ethernet),
- łatwe tworzenie sieci wirtualnych,
- realizacja funkcji mostu i routera,
- udoskonalenie w zarządzaniu siecią,
- bezpieczeństwo.

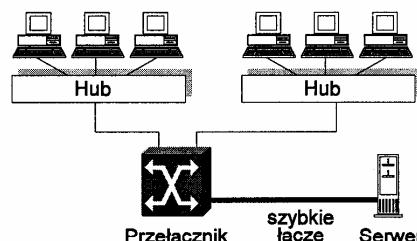
Niezawodność jest niezbędna ze względu na strategiczne miejsce (PCS), w którym znajduje się przełącznik. W celu tworzenia sieci wirtualnych przełączniki

muszą realizować funkcje mostu, routera, w tym dokonywać filtracji, wymaganej przez użytkowników.

Istota działania przełącznika polega na tworzeniu równoległych i równocześnie działających kanałów transmisji między parami portów przełącznika. Sieć z przełącznikiem jest bezpieczniejsza dla przesyłanych danych niż sieć ze wspólnym medium (Ethernet, Token Ring, FDDI).

## Przełącznik w grupie roboczej

Przelącznik w grupie roboczej eliminuje "wąskie gardło", jakim jest serwer wymagający dużej szybkości komunikacji (rysunek 9.31). Uzyskuje się to przez podłączenie serwera do jednego z wyjść przełącznika pracującego z dużą szybkością (np. 100 Mb/s). Do pozostałych wejść podłącza się huby (koncentratory).



Rys. 9.31. Przełącznik w grupie roboczej

Elastyczna architektura przełącznika pozwala na podłączenie maksymalnej liczby użytkowników oraz zapewnia łatwą współpracę z najszybszymi technologiami (FDDI, Fast Ethernet, ATM).

Skalowanie jest jeszcze bardziej efektywne, jeżeli bezpośrednio do wejścia przełącznika można podłączyć stacje sieciowe, a nie tylko huby. Segmentacja sieci jest wtedy najskuteczniejsza, a każdy użytkownik ma dostęp do dedykowanej szerokości pasma.

### 9.3.3.6 Zalety przełączników

Coraz popularniejsze przełączniki sieciowe charakteryzują się szeregiem niewątpliwych zalet. Należą do nich między innymi:

- obsługa dużej liczby portów (do 120);
  - obsługa dużej liczby adresów sieciowych dla jednego portu, dla przełączników grupowych (od 32 do 64 000), z tym że istnieją również przełączniki z przeznaczeniem dla pojedynczych stacji, obsługujące 1 adres na port;
  - szerokie spektrum agregowanych sieci, uzyskane dzięki dużej przepustowości magistrali łączącej porty, wymagane ze względu na możliwość

przyłączania wciąż rosnącej liczby sieci; szerokie spektrum oznacza zarówno dużą szybkość transmisji, jak i małe opóźnienia wprowadzane przez komutator/przełącznik;

- wbudowane mechanizmy zabezpieczające przed uszkodzeniami modułów lub portów (ang. *fault tolerant*): połączenia redundancyjne, zapasowy procesor(y), obsługujące przychodzące ramki, dodatkowe magistrale łączące porty, z automatycznym przełączeniem w przypadku uszkodzenia magistrali podstawowej, itp.;
  - wbudowane mechanizmy filtracji na poziomie podwarstwy MAC, z możliwością tworzenia wirtualnych podsieci jak i segmentacji sieci.

Integracja powyższych funkcji w jednym urządzeniu jest bardzo efektywnym rozwiązaniem. Ułatwia zarządzanie siecią, daje także znaczne oszczędności przy rekonfigurowaniu sieci w przypadku wystąpienia awarii. Dodatkowo pozwala na koncentrację serwerów w jednym miejscu, z dedykowaną przepustowością dla każdego z nich. Inną możliwością zwiększenia przepustowości do "farmy" serwerów jest zastosowanie wielu kart sieciowych, połączonych do przełączanych portów. Sterowanie ruchem realizowane jest wówczas przez oprogramowanie serwera. Elastyczna konfiguracja przełącznika pozwala na tworzenie odpowiedniej liczby wirtualnych podsieci, z dedykowaną dla nich przepustowością.

### 9.3.3.7 Sieci wirtualne VLAN

Pojawienie się przełączników stworzyło zupełnie nowe możliwości, jeśli chodzi o projektowanie i tworzenie sieci lokalnych. *Technika przełączania portów obsługujących poszczególne domeny rozgłoszeniowe pozwala, w przypadku zastosowania odpowiedniego przełącznika, tworzyć tzw. sieci wirtualne.* Definicja sieci wirtualnej nie została jak dotąd sformułowana przez żadną z poważnych organizacji standaryzacyjnych i generalnie można spotkać bardzo różne interpretacje tego pojęcia. Najbardziej trafną wydaje się definicja mówiąca, iż sieć wirtualna to zbiór stacji końcowych stanowiących pewną logiczną grupę, fizycznie rozproszoną po różnych segmentach pojedynczej sieci. Oznacza to, iż komputery będące w jednej sieci wirtualnej nie muszą współdzielić medium. Mogą być przyłączane do dwóch różnych segmentów, w dalszym ciągu stanowiąc jedną grupę (sieć wirtualną). Przynależność do różnych segmentów jest niezauważana dla użytkowników końcowych, również w aspekcie szybkości transmisji. Osiągnięcie dużych przepustowości pomiędzy dwoma, lub więcej, segmentami fizycznymi (domenami kolizyjnymi) możliwe jest tylko dzięki technice przełączania pakietów.

Generalnie przełączniki umożliwiają definiowanie sieci wirtualnych na jednym z trzech poziomów: na poziomie portów przełącznika, na poziomie adresów MAC komputerów należących do VLAN, na poziomie adresów warstwy sieciowej, np. adresów IP.

Pierwsza z tych metod na sztywno określa przynależność konkretnego portu przełącznika do jednej z sieci VLAN. Dołączanie kolejnych stacji do portu powoduje automatyczne rozszerzenie sieci wirtualnej. Rozwiązywanie to, stosunkowo proste w fazie definiowania i utrzymania sieci, staje się dosyć uciążliwe w momencie przekonfigurowywania sieci. Przełączanie stacji z jednej grupy roboczej (portu przełącznika) do drugiej powoduje automatyczną zmianę przynależności danej stacji do sieci wirtualnej, co nie zawsze musi być naszą intencją. Widać z tego, iż początkowa konfiguracja tego rodzaju sieci VLAN pozostaje niezmieniona i nie toleruje migracji stacji końcowych w ramach sieci LAN.

Druga technika polega na określeniu przynależności do konkretnej sieci wirtualnej na podstawie adresu MAC interfejsu sieciowego stacji roboczej. Tego rodzaju metoda posiada szereg zalet: po pierwsze fizyczne przeniesienie stacji (np. notebooka), z jednego segmentu/piętra do innego segmentu, nie zmusza administratora do żadnych dodatkowych operacji. Nakład pracy wniesiony w tym przypadku na początku konfigurowania sieci, a związany z dokładnym wpisaniem wszystkich adresów MAC wraz z ich przynależnością do określonego VLANa, opłaca się. Jedyną sytuacją, w której konieczna jest interwencja administratora, po wstępnej konfiguracji, jest dopisanie nowej stacji (jej adresu MAC) przybywającej do sieci VLAN. Jednym minusem sieci VLAN skonfigurowanej w oparciu o adres MAC jest brak odporności na stosowanie takich urządzeń jak docking stations. Są to „stacje logowania”, które posiadają zintegrowany interfejs sieciowy, a dostęp do sieci następuje przez fizyczne włożenie przenośnego komputera do takiej „docking station” co, niestety, oznacza identyfikację naszej stacji z adresem MAC stacji logowania, a nie komputera w niej rezydującego. Rozwiązyaniem w sytuacji używania docking stations jest zastosowanie techniki z grupowaniem portów.

Trzecia i ostatnia technika określania przynależności stacji do sieci wirtualnej oparta jest o unikatowy adres sieciowy. Obecnie, przełączniki znajdujące się na rynku wspierają takie protokoły jak IP, IPX, DECnet i AppleTalk. Przełączniki realizujące VLANy w oparciu o adres sieciowy są bardziej skomplikowane, bo docierają do trzeciej warstwy modelu odniesienia. Jednak to, iż operują w trzeciej warstwie nie oznacza, że w procesie przełączania angażują jakiekolwiek mechanizmy routingu pakietów. W zasadzie, oprócz tego, iż decyzja o przynależności pakietu do danej sieci wirtualnej podejmowana jest w oparciu o adres sieciowy a nie MAC-owy, nie ma wielkiej różnicy między tymi technikami. Oczywiście, duża przewaga sieci VLAN opartych o adresy sieciowe manifestuje się podwyższoną odpornością na fizyczne przemieszczanie się stacji roboczych, i większą odpornością na stosowanie urządzeń typu docking stations. Słabą stroną tej techniki jest dłuższy czas przełączania pakietów spowodowany koniecznością znalezienia adresu sieciowego wewnętrz pakietu, który w odróżnieniu od adresu MAC nie zawsze znajduje się w tym samym miejscu.

### 9.3.3.8 Podsumowanie

W ostatnim okresie czasu układy przełączające z powodzeniem wypierają dominujące do niedawna, przy łączeniu sieci LAN, mosty. Wynika to z faktu, że konstruowane w oparciu o nowe technologie przełączniki to urządzenia bardzo szybkie i gwarantujące praktycznie ciągły dostęp do określonego pasma przenoszenia. Istniejące obecnie przełączniki nie ograniczają się tylko do łączenia sieci pracujących w standardzie IEEE 802.3. Istnieją również przełączniki dla sieci realizowanych zgodnie z innymi standardami, jak np. Token Ring, Fast Ethernet, 100VG-AnyLAN, FDDI czy ATM. Coraz częściej spotykanym rozwiązaniem przełącznika jest układ integrujący kilka różnych przełączników, w jednej obudowie. Urządzenie takie, zwane koncentratorem, posiada, podobnie jak przełączniki ethernetowe, bardzo szybką magistralę wewnętrzną, poprzez którą mogą być przesyłane ramki, niezależnie od wybranej metody dostępu do medium. Moduły wymienialne przełącznika wieloprotokołowego muszą wówczas dokonywać poprawnej interpretacji ramek (pakietów), łącznie z ich filtracją i ewentualną konwersją (translakcją). Stosowanie przełączników wieloprotokołowych jest szczególnie przydatne w przypadku dużych sieci LAN, wykorzystujących sieci szkieletowe (np. wewnętrz budynków), do łączenia sieci LAN o różnych standardach. Połączenia pomiędzy budynkami realizowane są przy tym zwykle z wykorzystaniem szybkich łączów światłowodowych z przełączanym FDDI, 100VG -AnyLAN, czy też Fast Ethernetem.

### 9.3.4 Routery

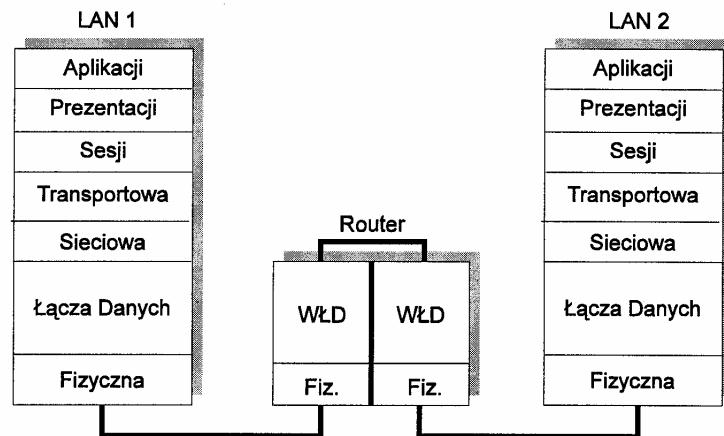
Routery są układami działającymi w warstwach fizycznej, łączących i sieciowej. Służą one do łączenia "rozległych" sieci LAN bądź sieci LAN i MAN z sieciami WAN, czy też sieci WAN między sobą. Router jest więc układem podobnym do mostu, jednakże z większym zakresem realizowanych funkcji. Należy tu zwrócić uwagę na fakt, że część mostów nazywana jest "brouterami" z uwagi na realizowane przez nie funkcje wyboru trasy.

#### 9.3.4.1 Zadania routerów

*Podstawowym zadaniem routera jest wybór właściwej trasy, wzduż której należy skierować pakiet. W tym celu router winien znać topologię sieci i realizować stosowne algorytmy wyboru trasy.* Z uwagi na znaczną złożoność i czasochłonność realizacji tych algorytmów również złożoność routera, w stosunku do mostu, czy przełącznika, znacznie rośnie. Jednocześnie maleje szybkość pracy routera (rozumiana jako liczba pakietów obsługiwanych przez router w jednostce czasu) w porównaniu z szybkością pracy sprzętowego mostu. Algorytmy wyboru trasy realizowane są bowiem programowo - w przeciwnieństwie do realizowanej sprzętowo funkcji filtracji i/lub konwersji formatów bądź enkapsulacji ramek. W przypadku sieci, nawet o identycznych architekturach logicznych, dopuszcza się różne formaty pakietów. Routery muszą wówczas dokonywać segmentacji/resegmentacji przesyłanych jednostek danych. Zadań tych nie realizują mosty.

Podstawowe funkcje routera wiążą się z obsługą jednostek danych warstwy trzeciej jednego (routery jednoprotokołowe) lub kilku (routery wieloprotokołowe) wybranych protokołów. Najczęściej spotykane są routery protokołów IP i IPX, rzadziej routery protokołów Banyan Vines, AppleTalk i DECnet.

Rysunek 9.32 przedstawia usytuowanie routera w modelu ISO.



Rys. 9.32. Router

Każdy z tych protokołów wymaga hierarchicznej struktury adresowania. Router przekazuje pakiety między poszczególnymi jednostkami adresacji, nazywanymi najczęściej sieciami, systemami autonomicznymi lub domenami. **Do wzajemnej komunikacji routery używają specjalizowanych protokołów**, dzięki czemu posiadają informacje o topologii sieci i możliwych do osiągnięcia sieciach lub domenach.

Routery skutecznie separamają łączone przez siebie sieci i efektywnie wyznaczają najlepsze drogi przesyłania danych. Do wad routerów trzeba zaliczyć ich wysoką cenę, spowodowaną koniecznością tworzenia odrebnego oprogramowania dla każdego typu protokołu oraz niższą, od mostów, sprawność, rozumianą jako liczba jednostek danych przesłanych w ciągu sekundy. Przyjmuje się, iż czas przebywania jednostki danych w routerze jest około dziesięciokrotnie dłuższy niż w moście.

Przy łączeniu wielu sieci komputerowych za pomocą „wspólnej” sieci szkieletowej (rdzeniowej) szczególnie popularne są routery wieloprotokołowe, wyposażone w oprogramowanie sieciowe szeregu standardowych architektur. Pakiety sieciowe pochodzące z różnych sieci, np. TCP/IP, OSI, SNA, DECnet, Novell, AppleTalk, itp. są w routerze dostosowywane do formatu pakietu obowiązującego w sieci szkieletowej. Realizowana jest wtedy zwykła procedura enkapsulacji tj. umieszczania pakietów, generowanych przez poszczególne sieci, jako dane, w strukturze

pakietu sieci szkieletowej. Z kolei w routerze docelowym odtwarzana jest pierwotna postać pakietu.

Routery są urządzeniami operującymi na adresach sieciowych. Sprawdzają one zatem zawarte w pakietach adresy by ustalić, czy napływające z sieci jednostki danych wymagają dalszej obsługi. Zwykle routery konstruują tablice wyboru tras pozwalające na efektywne kierowanie przepływem informacji. W przeciwieństwie do mostów, kierujących ramki dokładnie jedną trasą i najczęściej w sposób statyczny, routery mogą kierować pakiety wieloma trasami, dokonując dynamicznych modyfikacji tras. Routery dokonują też segmentacji i resegmentacji przesyłanych pakietów.

Z побieżnej analizy warstwowych architektur logicznych bądź sieciowych systemów operacyjnych NOS wynika, że producenci oprogramowania sieciowego proponują w tym zakresie różne rozwiązania. W przypadku sieciowych systemów operacyjnych novellowski NetWare używa protokołu IPX, IBM LAN korzysta z PC LAN Support Program, LAN Manager Microsoftu stosuje INTERNETowy IP. Oznacza to, że router, który łączy sieci funkcjonujące w oparciu o oprogramowanie Novella, IBM lub Microsoftu, musi obsługiwać co najmniej 3 powyższe protokoły komunikacyjne.

#### 9.3.4.2 Klasyfikacje routерów

W zależności od możliwości routera w zakresie protokołów komunikacyjnych warstwy łącza danych, routery mogą być kwalifikowane jako:

- routery uzależnione od protokołów (ang. *protocol dependent*) bądź
- routery niezależne od protokołów sieci (ang. *protocol independent*).

*Routery z "uzależnieniem" protokolarnym działają w środowisku wieloprotokołowym dokonując, przede wszystkim konwersji adresów do postaci obowiązującej w poszczególnych sieciach oraz zgodnie z wymaganiami protokołów komunikacyjnych implementowanych w sieciach źródłowych przesyłanych informacji.* Adres stacji docelowej zawarty jest w pakiecie źródłowym. Router dokonuje konwersji postaci pakietu - dodając adres kolejnego routera na trasie od sieci LAN źródłowej do sieci docelowej.

Wieloprotokołowe routery utrzymują oddzielne tablice tras dla każdego obsługiwanej protokołu. Wymaga to oczywiście znacznych pojemności pamięci oraz stosunkowo długiego czasu przetwarzania informacji protokolarno-adresowej. Czas ten staje się parametrem krytycznym w przypadku przesyłania informacji przez wiele routerów.

Router uzależniony od protokołu nie może być wykorzystywany do łączenia pewnych typów sieci LAN. Dotyczy to np. protokołów NETBIOS i IBM LAN Server, w których zamiast adresów stacji stosowane są nazwy. Tym samym pakiety, przesypane przez te sieci LAN, nie zawierają użytecznej dla wyboru trasy informacji adresowej.

**Routery niezależne od protokołów przypominają w swoim działaniu złożone funkcjonalnie mosty przeźroczyste.** Złożoność tych routerów wynika między innymi z faktu obsługi protokołów sieciowych sieci LAN, nie definiujących w zasadzie adresów sieciowych. Routery te badają adresy źródłowe stacji, w sieciach dołączonych do nich bezpośrednio, rozpoznając niejako automatycznie typy przyłączonych urządzeń końcowych. Router tego typu przyporządkowuje każdej sieci bez adresu sieciowego odpowiedni identyfikator. Pozwala to na jednoznaczną obsługę różnych typów pakietów i właściwe kierowanie ich wzdłuż wyznaczonych przez router tras.

Podobnie jak most przeźroczysty - router niezależny od protokołu sieciowego konstruuje tablice wyboru tras automatycznie, wymieniając informacje o tworzonych lokalnie tablicach z innymi routerami sieci. Zdolność do nauki topologii sieci w sposób istotny upraszcza administrowanie połączonym środowiskiem sieciowym. W przeciwieństwie do opisanej powyżej sytuacji zarządzanie siecią TCP/IP jest znacznie bardziej złożone. W sieci tej każda stacja robocza ma bowiem adres IP (internetowy) i musi znać adresy innych urządzeń LAN, z którymi chce nawiązywać łączność. Adresy te są przydzielane stacjom przez administratora. W przypadku zmiany lokalizacji lokalnej stacji jej adres IP ulega zmianie. Tym samym użytkownicy sieci muszą być powiadomieni o zmianach adresów stacji.

W przypadku łączenia kilku typów sieci za pośrednictwem wspólnej podsieci komunikacyjnej, pakiety z poszczególnych sieci mogą być „routowane” po uprzedniej ich enkapsulacji, do pakietu stosowanego w podsieci wspólnej.

W przypadku, gdy podsiecią tą jest sieć TCP/IP narzucająca stosowanie nagłówków o długościach 60 bajtów, metoda enkapsulacji może być jednakże bardzo nieefektywna. Dla przykładu, w sieci SNA przesyłane są zwykle krótkie pakiety o średniej długości 30 bajtów. Tym samym ich enkapsulacja ograniczałaby bardzo wyraźnie jakość pracy sieci. Rozwiążaniem korzystnym w przypadku obsługi mieszanego ruchu SNA i np. pochodzącego z sieci LAN TCP/IP jest stosowanie routera niezależnego od protokołów czyli routera przeźroczystego, który do każdego pakietu SNA będzie dodawał przydzielone, przez router, adresy LAN-owskie stacji źródłowej i docelowej będące np. adresami koncentratora i komputera komunikacyjnego sieci SNA.

W przypadku pakietów SNA będą one, po dotarciu do routera docelowego, rozpakowywane i w oryginalnej postaci dostarczane do adresata.

### 9.3.4.3 Protokoly wyboru tras

**Protokół routingu** (ang. *routing protocol*) jest metodą, zgodnie z którą router dokonuje wyboru trasy i wymienia informacje z innymi routerami bądź przyłączonymi do niego sieciami. Protokół wyboru trasy ma wpływ zarówno na efektywność funkcjonowania sieci, jak też wymagania odnośnie pamięci routera.

#### 9.3.4.3.1 Algorytmy i tablice routingu

W procesie przekazywania danych poprzez „intersieć” ważną rolę odgrywają routery. Samą nazwę „router” można tłumaczyć jako urządzenie wyznaczające „marszrutę” (trasę) połączenia.

Router jest komputerem, często specjalnie zaprojektowanym do realizacji funkcji routingu, chociaż może to być również „zwykły” komputer z zaimplementowanym w nim oprogramowaniem realizującym te funkcje (np. program *routed* w systemie UNIX).

Wyznaczanie trasy pakietów jest procesem stosunkowo złożonym. Do tego celu stosuje się różnorodne algorytmy routingu, optymalizujące ogólnie rozumiany koszt całego połączenia, przyjmując przy tym różne metryki charakteryzujące koszty poszczególnych połączeń. Takimi metrykami mogą być: liczba routerów, przez które przechodzi dana trasa, opóźnienie wnoszone przez daną trasę, przepustowość trasy, „fizyczny” koszt połączenia. Różne algorytmy routingu mogą więc wybrać różne trasy jako optymalne - zależnie od rodzaju użytych metryk i samego algorytmu wyboru trasy. Wybór algorytmu routingu zależy od rodzajów łączonych sieci, ich konfiguracji, a także rozmiaru.

Żeby sprawnie kierować ruchem pakietów, routery tworzą specjalne tablice routingu, które zawierają informacje o trasach. Są to zazwyczaj informacje o trasach do poszczególnych sieci, a nie pojedynczych komputerów. Zmniejsza to zasadniczo rozmiary tablic routingu. To, jakie informacje gromadzone są przez routery, zależy od realizowanego algorytmu wyboru trasy. Najczęściej tablice organizowane są jako zbiory par parametrów, z których pierwszym elementem jest numer sieci docelowej. Poniżej przedstawiamy przykłady „par” z tablic routingu:

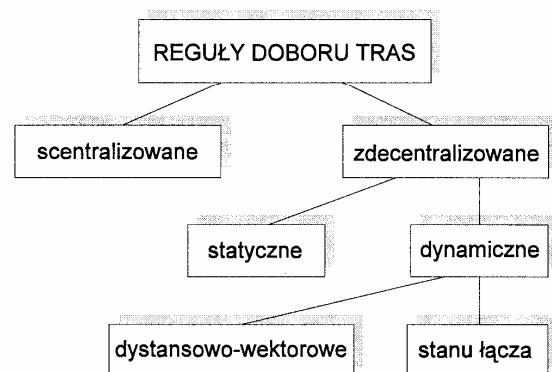
1. Parę: <adres sieci przeznaczenia, następny etap>. To powiązanie wskazuje następne ognisko na drodze do sieci określonej przez adres przeznaczenia. Jeśli chcemy przesłać pakiet pod dany adres przeznaczenia trasą optymalną, to należy wysłać ten pakiet do kolejnego routera, nazywanego tutaj następnym etapem (ang. *next hop*). Przykład takiej tablicy przedstawia tabela 9.3.

Tab. 9.3. Przykład tablicy routingu

sieć docelowa	następny etap	koszt
12	bezpośrednia	0
43	routera 1	1
32	routera 2	2
27	routera 3	5
10	routera 4	2
11	routera 1	3

2. Pary: <adres sieci przeznaczenia, metryka połączenia>. To powiązanie wskazuje, że sieć docelowa jest odległa od routera źródłowego (w sensie danej metryki) o wartość określona przez podaną metryką. Router porównuje metryki, żeby wyznaczyć optymalną trasę.
3. Pary: <adres sieci przeznaczenia, numer ścieżki>. Żeby osiągnąć sieć docelową, trzeba wybrać określoną ścieżkę. W tym przypadku routery przekazują pakiety wzdułej tej ścieżki, aż dotrą one do sieci przeznaczenia.

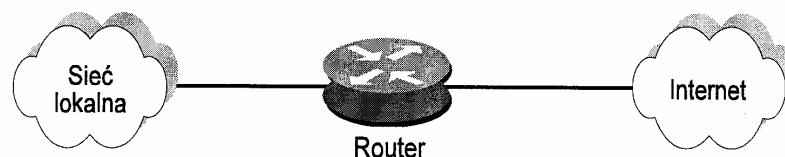
Dokonując uproszczonej klasyfikacji metod routingu, procedury wyboru trasy dzielimy zwykle na scentralizowane bądź zdecentralizowane. Te dzielimy zazwyczaj na statyczne (sztywne) i dynamiczne. Algorytmy statyczne nie uwzględniają informacji o zmianach zachodzących w sieci i opierają swoje decyzje na informacjach uzyskiwanych przez router w chwili inicjowania jego pracy w sieci. W przypadku algorytmów dynamicznych router bierze pod uwagę zmiany zachodzące w obciążeniu i/lub topologii sieci. W obu przypadkach możliwe jest też dalsze definiowanie podklaś metod routingu. Przykład klasyfikacji reguł doboru tras podano na rysunku 9.33.



Rys. 9.33. Klasyfikacje reguł doboru tras

W przypadku **routingu statycznego** tablice routingu są konstruowane przez administratorów sieci. Ten typ routingu może być użyty w sieci, gdzie trasy przekazywania danych nie zmieniają się zbyt często. Zwykle tablice statyczne routingu stosuje się w tych miejscach, gdzie istnieje tylko jedna trasa do innych sieci; mogą to być tzw. liście sieci. Są to przeważnie sieci LAN łączone przez jeden router (lub kilka routerów) z większą siecią, np. Internetem. Przykład takiej konfiguracji pokazuje rysunek 9.34. W tym przypadku router musi posiadać w tablicy routingu pozycje wskazujące trasy do komputerów w tej sieci lokalnej oraz jedną pozycję z trasą domyślną do innych adresatów tzn. stacji znajdujących się poza

tą siecią. Jeśli jakiś komputer z tej sieci lokalnej będzie chciał przesyłać pakiet do innej sieci, to router po odebraniu tego pakietu prześle go trasą domyślną do Internetu.



Rys. 9.34. Ilustracja do łączenia sieci LAN do sieci Internet za pośrednictwem routera

W obecnie działających dużych sieciach trasy zmieniają się dość często, np. z powodu uszkodzeń i/lub zmennego obciążenia. W tym przypadku człowiek nie jest w stanie nadążyć z wykrywaniem zmian i „ręczną” zmianą tablic w każdym routerze. Dlatego też szczególnego znaczenia nabiera **routing dynamiczny**, który umożliwia szybkie zmiany tras w zależności od warunków pracy sieci. Tablice routingu są wtedy budowane dynamicznie z uwzględnieniem informacji pomocniczych o stanie sieci między routerami. Takie rozwiązanie stosuje się w dużych sieciach, gdzie wiele tras może prowadzić do tego samego miejsca docelowego. Dzięki protokołom routingu można wtedy określić trasę najlepszą, ale też w przypadku jej uszkodzenia można szybko znaleźć trasę zastępczą.

Jak wspomniano, jedną z podstawowych cech routingu dynamicznego jest wymiana informacji o trasach, dokonywana między routerami. Odbywa się to za pośrednictwem specjalnych komunikatów. Przykładem takiego komunikatu może być wiadomość typu *routing update message*. Zawiera ona zwykle albo całą tablicę routingu, albo jej część. Router, dzięki informacjom o trasach, uzyskanym od innych routerów, może wyznaczyć trasy optymalne. Komunikaty *routing update message* są wysyłane albo regularnie albo tylko wtedy, gdy następują zmiany w topologii sieci.

Routery mogą też wymieniać między sobą komunikaty typu *link-state advertisement*, które informują o stanie łączy, routera nadawcy, z innymi routerami. Informacja o stanie łączy może być wykorzystana do budowy mapy połączeń między routerami i sieciami. Na podstawie tej mapy routery mogą określać optymalne trasy.

Wśród protokołów routingu dynamicznego wyróżnia się dwie podstawowe klasy algorytmów. Są to:

- **algorytmy wektorowo-odległościowe** (bądź dystansowo-wektorowe) (ang. *distance-vector*) - W przypadku tych algorytmów decyzje o wyborze trasy podejmowane są w oparciu o odległość do poszczególnych sieci lub koszt związany z przesłaniem pakietu po danej trasie. Informacje do wyznaczenia tras są przesyłane za pośrednictwem komunikatów *routing update message*. Routery pracujące wg. tego algorytmu mają

w tablicach routingu informacje nie tylko o tym, jaki router trzeba użyć do przesyłania pakietu do celu, ale także o koszcie trasy (patrz przykładowa tablica routingu przedstawiona w tablicy 9.3). Nazwa „wektor-odległość” wynika z tego, że komunikaty zawierają zbiory par (W,O), gdzie W określa cel - nazywany wektorem, a O - odległość do tego celu. Początkowo, router wypełnia tablice routingu pozycjami zawierającymi informacje o sieciach bezpośrednio do niego dołączonych i ustawia dla nich odległość 0. Okresowo router wysyła do innych, bezpośrednio z nim połączonych, routerów komunikaty *routing update message*, zawierające własną tablicę routingu. Gdy do routera X dotrze komunikat od routera Y, to analizuje on zbiór adresów docelowych jakie można osiągnąć poprzez router Y i odległości do tych „celów”. Jeśli okaże się, że router Y zna krótszą trasę do „celu” lub gdy Y podaje informacje o trasie, której X nie ma jeszcze w swojej tablicy, to router X zmienia zawartość swojej tablicy routingu. Zmiana jest dokonywana także w przypadku, gdy X używa trasy przechodzącej przez Y do jakiegoś „celu” i następuje zmiana odległości Y od tego celu. Jeśli X wpisuje do swojej tablicy trasę przechodzącą przez Y, to odległość zapisana w jego tablicy jest zwiększona o 1 w stosunku do odległości podanej przez Y. Algorytmy typu wektor-odległość są łatwe w implementacji. Nie nadają się jednak do dużych sieci, w których występują częste zmiany w konfiguracji. Algorytmy takie są bowiem wolnozbieżne. Zbieżność w tym wypadku określamy jako proces ustalania takich samych optymalnych tras przez wszystkie routery, po wystąpieniu zmiany w topologii. Gdy zmienia się trasa, informacje o zmianie „przemieszczają się” dość wolno, i niektóre routery mogą mieć niepoprawne informacje. Może to powodować powstawanie tymczasowych pętli. Dlatego też algorytmy te mogą być używane tylko w sieciach, w których zmiany nie zachodzą zbyt często. Wadą algorytmów dystansowo-wektorowych jest też i to, że wymagają one przesyłania długich komunikatów. Komunikaty muszą bowiem zawierać informacje o wszystkich sieciach docelowych, są więc zależne od rozmiaru intersieci. Algorytmy takie rozsyłają komunikaty zwykle periodycznie. Zatem dla tego przy dużych intersieciach ruch związany z wymianą informacji o trasach może być bardzo duży.

- **algorytmy stanu łącza** (połączenia) lub najkrótszych ścieżek (ang. *link-state algorithm* lub *Shortest Path First* (SPF - najpierw najkrótsza ścieżka)). Algorytmy tego typu wymagają większego nakładu na przetwarzanie niż algorytmy typu wektorowo-odległościowego, jednakże umożliwiają efektywniejszą kontrolę procesu routingu. W protokołach tego typu każdy router w sieci tworzy bazę danych opisującą topografię całej intersieci, tj. pokazującą wszystkie inne routery, sieci i ich wzajemne połączenia. Poszczególne routery posiadają identyczne bazy da-

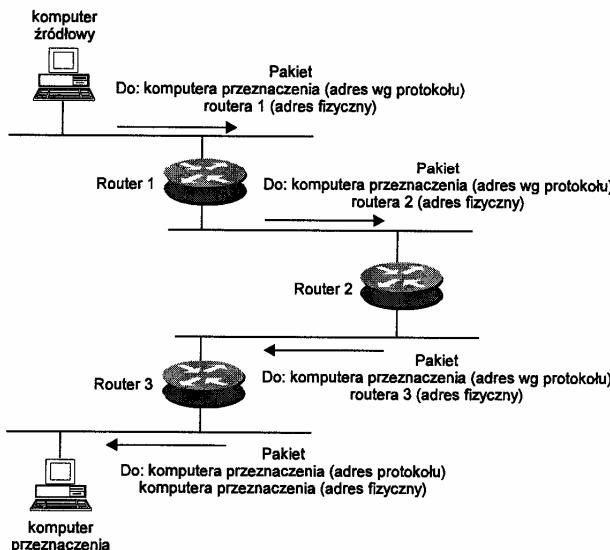
nych. Każda pozycja w takiej bazie zawiera informacje o stanie innych routerów, tzn. o stanach ich interfejsów i osiągalnych sąsiadach. Każdy router testuje stan wszystkich sąsiadujących z nim routerów i rozsyła informacje o stanie swoich połączeń do wszystkich pozostałych routerów. Są to komunikaty typu *link-state advertisement*. Na podstawie tych informacji routery tworzą i modyfikują mapę intersieci oraz wyznaczają drzewa najkrótszych tras, ustalając siebie jako korzenie. Do tego celu wszystkie routery używają jednego ze znanych algorytmów, np. algorytmu Dijkstry, znajdowania najkrótszych ścieżek w grafie połączeń. Zaletą tego typu algorytmów jest to, że każdy router wyznacza trasy niezależnie, na podstawie tych samych danych; proces taki jest więc zbieżny. W przypadku algorytmów „stanu łączy” komunikaty przesyłane między routerami zawierają tylko informacje o stanie łączy poszczególnych routerów, a nie o stanie wszystkich sieci docelowych, jak to jest w przypadku algorytmów wektorowo-odległościowych. Zatem rozmiary tych komunikatów nie zależą od rozmiaru intersieci. Z uwagi na to, że routery korzystają z tych samych danych i stosują te same algorytmy wyznaczania tras najkrótszych, w sieci nie występują pętle. Jeżeli określony węzeł A leży na trasie najkrótszej (czytaj o najmniejszym koszcie) prowadzącej z routera X do Y, wyznaczonej w X, to oczywiście trasa najkrótsza z A do Y, określona w A, będzie częścią tej samej trasy (z X do Y). W każdym routerze, na podstawie wyznaczonych tras o najmniejszych kosztach, możemy więc skonstruować tablicę kierunków, podobną do stosowanej w przypadku realizacji algorytmów ze sztywnym wyborem tras. Gwarantuje to poruszanie się pakietów po trasach o najmniejszym koszcie (najkrótszych). Aktualizacja tablic kierunków dokonywana jest bądź określowo bądź w chwilach, w których występują istotne zmiany wartości kosztów, względnie struktury sieci, na skutek awarii.

Algorytmy routingu używane w sieciach komputerowych, są dokładnie wstępnie określone i nazywa się je protokołami routingu. Specyfikacje takich protokołów określają między innymi, jakiego rodzaju komunikaty są wymieniane pomiędzy routery, jaka jest ich zawartość oraz jak określana jest trasa optymalna. Zawierają one też i inne parametry, specyficzne dla danego protokołu.

Samo przekazywanie danych między sieciami (po angielsku określone często jako „switching in the 3rd layer”, tzn. przełączanie w warstwie 3) jest raczej prosty. Proces ten dla wielu algorytmów routingu przebiega bardzo podobnie. W przypadku, gdy tablice routingu zawierają pary <adres przeznaczenia, następny etap> algorytm ten możemy przeledzić na prostym przykładzie.

Załóżmy, że komputer źródłowy chce przesłać pakiet do innego komputera (komputera przeznaczenia). Jeśli komputer przeznaczenia jest w tej samej sieci co komputer źródłowy, to komputer źródłowy wysyła do niego pakiet bezpośrednio, używając adresu fizycznego (tj. adresu warstwy MAC - urządzenia sieci LAN).

W przypadku, gdy komputer docelowy znajduje się w innej sieci, to komputer źródłowy kieruje pakiet do znanego mu routera z adresem fizycznym tego routera i z adresem sieciowym komputera przeznaczenia. Router, po otrzymaniu pakietu, sprawdza w tablicy routingu, dokąd ma przesyłać odebrany pakiet. Jeśli nie ma stosownej informacji, to zazwyczaj odrzuca pakiet. Jeśli jednak dysponuje informacją, do którego z sąsiednich routerów powinien przesyłać pakiet, to zmienia adres fizyczny, zawarty w pakiecie, na adres fizyczny tego routera i przesyła do niego pakiet. Gdy pakiet dotrze do ostatniego routera znajdującego się na trasie do komputera przeznaczenia, to router ten identyfikuje, na podstawie adresu sieciowego, jedną z bezpośrednio dołączonych do niego sieci i przesyła pakiet do komputera przeznaczenia, umieszczając w pakiecie adres fizyczny, odpowiadający temu komputerowi. Opisany powyżej proces ilustruje rysunek 9.35. Jak widać z rysunku oraz z powyższego opisu, pakiet ma cały czas ten sam adres sieciowy, zmieniany jest tylko zawarty w nim adres fizyczny, zgodnie z adresami MAC kolejnych węzłów znajdujących się na trasie do komputera przeznaczenia.



Rys. 9.35. Przekazywanie danych poprzez routery

#### 9.3.4.3.2 Routing w sieciach TCP/IP

Podstawową usługą Internetu jest przekaz pakietów pomiędzy połączonymi sieciami. W przypadku sieci TCP/IP definiowany jest protokół datagramowy Internet Protocol (IP). Realizuje on bezpołączeniowy przekaz informacji, zgodnie z popularną zasadą "best - effort", czyli po prostu - zrobię wszystko co w mojej mocy, ale nie wymagaj zbyt wiele.

Poszczególne pakiety mogą więc być tracone, mogą pojawiać się ich duplikaty, zmiana może ulegać kolejność ich dostarczania do adresata, a samo ich dostarczenie może być opóźnione. Usługa świadczona przez warstwę sieciową jest więc wysoce zawodna.

Protokół IP, najpowszechniej w praktyce stosowany algorytm współpracy sieci pakietowych, definiuje

- jednostki danych przekazywane poprzez TCP/IP Internet,
- funkcje routingu,
- zespół mechanizmów i zasad pozwalających na efektywny przekaz pakietów.

Zasady te charakteryzują sposób przetwarzania pakietów w węzłach i routeraх sieci, metody generacji informacji sterujących oraz warunki, przy których następuje usunięcie pakietu z sieci.

Do celów routingu wykorzystywane są głównie pola adresowe datagramu. Decyzje o wyborze trasy podejmowane są jednakże z wykorzystaniem i innych pól pakietu. Do tego celu służą również bity pola typu usługi. W zależności od żądanej jakości przekazu informacji, router może dokonywać wyboru, np. pomiędzy łączami dzierżawionymi o niskiej przepustowości, a łączami satelitarnymi o wysokiej szybkości transmisji. W przypadku przesyłania informacji pomiędzy odmiennymi fizycznie sieciami TCP/IP, stosowana jest metoda enkapsulacji datagramów. Idealnym rozwiązaniem jest umieszczenie całego datagramu w jednej ramce. Najczęściej jednakże dochodzi do podziału datagramu na segmenty. Fakt przenoszenia datagramu IP w ramce danej sieci jest odpowiednio sygnalizowany. W przypadku sieci Ethernet proces enkapsulacji jest specyfikowany w polu typu ramki. Pożądane jest przy tym tworzenie, po stronie źródłowej wiadomości, datagramów o długościach dostosowanych do wymiarów ramek w sieciach, poprzez które datagram winien być przesyłany. Z uwagi na złożoność tego zagadnienia, a jednocześnie konieczność ukrycia przed użytkownikiem technologii poszczególnych sieci Internetu, fragmentacja (podział) datagramu dokonywana jest przez routery funkcjonujące na "granicach" sieci składowych internetu. Tym samym protokół IP nie narzuca ograniczeń na rozmiary datagramów (z wyjątkiem wymiaru maksymalnego). Ważną cechą protokołu IP jest to, że po podziale na mniejsze fragmenty, zmodyfikowane datagramy są transmitowane dalej, do ich miejsca przeznaczenia, niezależnie. Niewątpliwa zaletą tego rozwiązania jest jednakże eliminacja uciążliwości ponownego odtwarzania datagramu przez ściśle określony router "wyjściowy" sieci.

Routing w sieciach TCP/IP odbywa się aktualnie w oparciu o 32 bitowe adresy IP (IPv4) stacji źródłowej i docelowej. Router dokonuje przy tym wyboru trasy najbliższej. Przy podejmowaniu decyzji wykorzystuje przechowywaną w jego pamięci tablicę wyboru tras. Tablice wymieniane pomiędzy routerami określonego poziomu są okresowo modyfikowane.

Protokół IP definiuje też szereg ciekawych dodatkowych opcji. Jedna z nich dotyczy odmiennej, od wspomnianej powyżej, zasady routingu. IP dopuszcza bowiem tzw. routing źródłowy. Zgodnie z zasadą tego routingu to stacja nadawcza datagramu określa trasę, wzdłuż której ma być on przesyłany. Zastosowanie opcji z routinem źródłowym może być uzasadnione potrzebą przetestowania, przez administratora określonej sieci, możliwości transmisyjnych pewnego fragmentu internetu. Specyfikowane są przy tym dwie wersje routingu źródłowego.

- pełny routing źródłowy (o zasadzie identycznej do stosowanego przy łączaniu sieci IBM Token Ring (IEEE 802.5) i
- częściowy routing źródłowy, w którym nadawca określa jedynie ciąg adresów sieciowych routerów, nie zawsze sąsiednich; w tym przypadku możliwe jest rozsyłanie datagramu wieloma trasami między wskazanymi routerami.

### **Wpływ adresacji na routing w Internecie**

Kluczową rolę w wyznaczaniu tras datagramów i przy przesyłaniu datagramów wzdłuż tych tras odgrywają adresy sieciowe stacji.

Adres IP składa się z dwóch części (por. paragraf 1.3.4):

- części sieciowej i
- części określającej port w danej sieci.

Bardzo często mówi się, że druga część adresu identyfikuje komputer. Zwykle bowiem z określonym komputerem związany jest tylko jeden port. Zdarza się jednak, iż komputer może mieć kilka portów i kilka związanych z nimi adresów IP. Przykładem takiego komputera jest router.

Ponieważ schemat adresacji dzieli adres na część sieciową i numer portu (komputera), tablice routingu mogą zawierać informacje o trasach do sieci, a nie do poszczególnych routerów. Umożliwia to znaczone zmniejszenie rozmiarów tych tablic.

Podział adresu na dwie części upraszcza zasady administrowania adresami w sieci Internet. Specjalnie powołana do tego celu organizacja Internet Network Information Center (INTERNIC) zajmuje się tylko przydziałem części sieciowych adresów IP. Natomiast poszczególne ośrodki same rozdzielają adresy wewnętrz w sieci, zgodnie z prowadzoną przez siebie polityką.

Obowiązujący w Internecie 32-bitowy schemat adresacji ma wiele wad. Kiedy był on tworzony, dominowały kosztowne i wielkie superkomputery. Nikt nie przewidywał wówczas takiej powszechności komputerów osobistych. Projektanci zakładali wtedy, że będzie istniało niewiele dużych sieci. Dlatego też stworzono klasę A sieci przydzielając jej połowę przestrzeni adresowej. Z czasem jednak, wraz z rozwojem Internetu okazało się, że największe zapotrzebowanie zgłaszanego jest na adresy klasy B i C (por. paragraf 1.3.4). Bardzo poważną wadą okazał się też sztywny podział adresów na klasy. Przykładowo, przydzielenie adresu klasy B sieci organizacji, która nigdy nie będzie miała 65 tysięcy komputerów, spowoduje,

że większość adresów w tej sieci nie zostanie wykorzystanych. Ponieważ adresów klasy B jest mało, a liczba wolnych adresów tej klasy jest coraz mniejsza, coraz trudniej jest taki adres uzyskać. Z drugiej strony przydzielenie kilku lub kilkudziesięciu adresów klasy C powoduje drastyczny wzrost informacji zawartych w tablicach routingu (w routeraх).

Z powyższych względów istnieje pilna potrzeba wprowadzenia nowej wersji protokołu IP z większą przestrzenią adresową (IPv6). Zanim jednak zostanie ona wprowadzona do powszechnego użytku, niezbędne są mechanizmy tymczasowe pozwalające na doraźne ograniczenie powyższych niedostatków adresacji w Internecie.

#### **9.3.4.3.2.1 Podsieci**

Jednym z udogodnień adresacji w protokole IP było wprowadzenie pojęcia podsieci. Podsieci zdefiniowano w połowie lat 80. Strukturę adresów IP można lokalnie modyfikować poprzez użycie bitów adresowych komputera jako dodatkowych bitów określających sieć. W tym celu część adresu komputera dzieli się na część identyfikującą podsieci i część identyfikującą sam komputer (port). Sposób podziału nie jest sztywny; „linia podziału” jest przesuwalna i jest określana przez specjalną 32 bitową maskę, zwana maską podsieci. Interpretację adresu IP uzyskuje się poprzez przyłożenie maski podsieci i adresu IP. Jeśli bit w masce podsieci jest jedynką, to odpowiadający mu bit w adresie IP jest interpretowany jako bit adresu podsieci. W przeciwnym przypadku, to znaczy, gdy bit w masce równy jest zero, to odpowiadający mu bit adresu IP należy do części identyfikującej komputer. Zilustrujemy to przykładem. Niech adres IP komputera jest równy 153.19.170.143 i używa on maski podsieci 255.255.255.0. Jak widać jest to adres klasy B i sieć, do której należy ten komputer, ma adres 153.19.0.0. Ponieważ jednak została użyta maska podsieci, to 3 bajt adresu nie identyfikuje komputera, tylko dodatkowo podsieci. Zatem adres podsieci jest 153.19.170.0.

Wprowadzenie podsieci umożliwia organizacjom dzielenie własnej sieci na jeszcze mniejsze obszary, bez obowiązku zgłoszenia ich do INTERNIC. Jednocześnie routing do takiej sieci będzie przebiegał bez zmian. Routery znajdujące się poza tą siecią będą do niej przesyłać datagramy nie wiedząc nawet o fakcie istnienia podsieci. Tak więc podział na podsieci nie wpływa na zwiększenie rozmiarów tablic routingu w routeraх znajdujących się poza tą siecią. Dopiero routery wewnętrz tej sieci będą interpretować część identyfikującą podsieci i przesyłać datagramy do odpowiednich podsieci. Muszą one zawierać specjalne tablice routingu określające trasy do podsieci. Tablica routingu w takim przypadku będzie zawierała trójkę elementów:

- adres podsieci,
- maskę bitową skojarzoną z tą siecią,
- adres następnego etapu.

### 9.3.4.3.2.2 Nadsieci

Drugim używanym rozwiązaniem jest definiowanie tzw. nadsieci. Idea nadsieci jest analogiczna jak podsieci, z tym, że w tym przypadku mamy do czynienia z łączeniem wielu adresów sieci i traktowaniu ich jako adresów jednej sieci. Przyczyną wprowadzenia nadsieci było wyczerpywanie się liczby dostępnych adresów sieci klasy B, przy dużej liczbie wolnych adresów klasy C. Stwierdzono, że można przydzielać organizacjom bloki adresów C, zamiast adresu klasy B. Przydzielanie wielu adresów klasy C powoduje jednak wzrost rozmiarów tablic routingu. Dlatego zastosowano nową metodę routingu bezklasowego CIDR (ang. *Classless Inter-Domain Routing*). Metoda ta polega na przypisaniu blokowi adresów tylko jednego adresu przeznaczenia w tablicy routingu. Tak samo jak w przypadku podsieci, wymaga to modyfikacji sposobu routingu w routerach i w protokołach routingu. Routerzy powinny obsługiwać te adresy jako bezklasowe tzn. nie wyznaczać tras na podstawie adresów sieci klasy A, B lub C tylko na podstawie prefiksu adresu sieci wraz z liczbą określającą długość prefiksu. Przykładem takiego adresu jest 192.32.0.0/16, gdzie 192.32.0.0 oznacza prefiks adresu, a liczba 16 definiuje długość prefiksu w bitach. Taki sposób adresacji pozwala na dowolne łączenie wielu adresów w jeden, np. podany powyżej prefiks adresu oznacza adresy sieci klasy C od 192.32.0.0 do 192.32.255.0.

### 9.3.4.3.2.3 Protokoły routingu stosowane w sieciach TCP/IP

Protokół internetowy IP nie definiuje zasad kierowania ruchem datagramów ani w danej domenie (sieci autonomicznej) ani też między domenami. Z tego też względu w sieci TCP/IP opracowano szereg protokołów wyboru tras. Przesyłanie datagramów z jednego komputera do innego, odległego komputera w sieci, odbywa się z użyciem routerów.

Gdy komputer chce wysłać datagram, sprawdza najpierw czy komputer docelowy znajduje się w tej samej sieci. W tym celu porównuje adres swojej sieci z adresem sieci komputera przeznaczenia.

Jeśli w danej sieci definiowane są podsieci, to do adresu przeznaczenia, zgodnie z koncepcją tworzenia podsieci, stosowana jest maska podsieci. Jeśli komputer docelowy znajduje się w tej samej sieci (podsieci) co komputer źródłowy, to komputer źródłowy wysyła datagram bezpośrednio do adresata, po umieszczeniu datagramu we właściwym formacie ramki. Adres MAC adresata pozyskiwany jest na podstawie znanego adresu IP, np. za pomocą protokołu ARP (por. 1.3.4).

Jeśli komputer docelowy znajduje się w innej sieci, to datagram jest przesyłany do routera.

Router po odebraniu datagramu podejmuje stosowne działania:

- sprawdza adres IP odbiorcy,
- wyznacza adres sieci docelowej (ASD). Jeśli ASD zgadza się z adresem którejś z bezpośrednio dołączonych sieci, to dostarcza datagram za po-

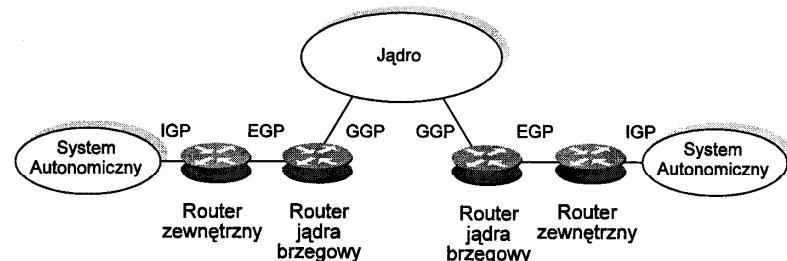
mocą tej sieci, stosując przy tym protokół ARP i enkapsulację datagramu. W przeciwnym przypadku, dla każdej pozycji w tablicy routingu (1-wsza pozycja zawiera maskę podsieci, a dalsze - adres podsieci oraz adres następnego etapu) wykonuje iloczyn logiczny maski podsieci i adresu odbiorcy (AO) i przesyła datagram pod wskazany adres następnego etapu.

### Pierwotna architektura routingu w Internecie

W początkowej fazie tworzenia Internetu, sieć ARPANET była szkieletem całej sieci. Z tego powodu przyjęto pewną hierarchię sieci wynikającą z początkowej struktury Internetu. Zdecydowano więc, że sieć będzie się składała z:

- jądra i
- systemów autonomicznych (zwanych często domenami).

Koncepcję tę obrazuje rysunek 9.36.



Rys. 9.36. Hierarchia routerów

Jądro czy też szkieletem była oczywiście sieć ARPANET. Jądro zawierało grupę routerów centralnych, nazywanych routerami jądra (inne określenie to routery podstawowe), które dysponowały pełną informacją o Internecie. Z kolei System Autonomiczny (SA - ang. *Autonomous System* - AS) to zbiór wielu sieci i routerów zarządzany przez jedną organizację i stosujący jeden mechanizm gromadzenia informacji o trasach i zasadach ich wyznaczania. SA realizuje więc na swoim obszarze wspólny protokół routingu. Protokół taki nazywamy jest wewnętrznym protokołem routingu (ang. IGP - *Interior Gateway Protocol*). Istnieją różne wewnętrzne protokoły routingu - najbardziej znane to RIP, OSPF, Hello, IS-IS i EIGRP. Pierwszy z nich zaliczany jest do klasy protokołów dystansowo-wektorowych, drugi natomiast - do protokołów stanu łączna. System autonomiczny ma zawsze przynajmniej jeden router, który przekazuje do systemu routerów jądra informację o osiągalności SA, tzn. informację o tym, jakie sieci są dostępne przez dany system autonomiczny. Na podstawie tych danych routery jądra wyznaczają trasy do każdego miejsca w sieci. Routery jądra przetwarzają i wymieniają dane między sobą za pomocą protokołu GGP (ang. *Gateway-to-Gateway Protocol*). Natomiast routery zewnętrzne (łączące systemy autonomiczne między sobą lub z jądrem)

używają protokołu EGP (ang. *Exterior Gateway Protocol*) do przekazywania informacji o osiągalności innych sieci. Jednocześnie router zewnętrzny używa wewnętrznego protokołu routingu, aby uzyskiwać informacje o trasach we własnym systemie autonomicznym. Według powyższej definicji systemu autonomicznego, jądro jest także systemem autonomicznym, z tą różnicą, że routery jądra nie przekazują informacji tylko o sieciach w jądrze, ale o wszystkich sieciach w Internecie, czego nie mogą robić routery zewnętrzne.

#### **Gateway to Gateway Protocol**

Protokół GGP, opisany w RFC 823, był używany przez routery jądra do wymiany między sobą informacji o trasach w sieci. Jest to protokół typu wektorowo-odległościowego. Informacje przesyłane przez routery w protokole GGP to pary (adres sieci, odległość). Jako miarę odległości w GGP przyjęto liczbę etapów transmisji mówiącą, ile routerów znajduje się na trasie datagramu do określonej sieci docelowej. W przypadku sieci dołączonych do routera bezpośrednio, router przyjmował liczbę etapów równą 0. Stosowane w protokole komunikaty routinguowe były umieszczane w datagramach IP. Komunikaty GGP miały nagłówek o ustalonym formacie, który identyfikował typ komunikatu i format pozostałych pól. GGP definiował następujące typy komunikatów:

- **Zmiana trasy** - Komunikat ten zawierał informacje o odległościach routera nadającego do innych sieci, przy czym informacje te były pogrupowane wg. odległości. Oprócz tego komunikat zawierał pole z numerem porządkowym, które służyło do zapewnienia integralności przesyłanych danych (tzw. *sequencing*). Jedno z pól dodatkowych służyło do przesłania od odbiorcy komunikatu o zmianach w jego tablicy.
- **Potwierdzenie żądania** - Komunikat ten zawierał potwierdzenie pozytywne lub negatywne odbioru komunikatu o zmianie trasy. Komunikat ten zawierał także numer porządkowy.
- **Prośba o echo** - Komunikat wysyłany w celu sprawdzenia, czy jest łączność z innym routерem.
- **Odpowiedź na echo** - Komunikat będący odpowiedzią na komunikat typu „prośba o echo”.

Po zmianie struktury organizacyjnej Internetu protokół ten nie jest już wykorzystywany. Jego znaczenie jest zatem wyłącznie historyczne (i dydaktyczne!).

#### **Exterior Gateway Protocol**

Router, w którym zaimplementowano protokół EGP, udostępnia informacje o sieciach, które są osiągalne w jego systemie autonomicznym. Protokół ten umożliwia też informowanie o sieciach spoza własnego systemu autonomicznego, jednak mogą to robić tylko routery jądra. Routery zewnętrzne mogą jedynie informować o własnych sieciach. Protokół ten określa dwa komunikujące się, przy jego użyciu, routery mianem sąsiadów, przy czym, jeśli należą oni do tego samego systemu

autonomicznego, to są to sąsiedzi wewnętrzni, w przeciwnym wypadku są to sąsiedzi zewnętrzni. Każdy komunikat EGP ma nagłówek zawierający informację o wersji protokołu EGP, typie komunikatu, jego kodzie (określa podtyp), stanie, numerze systemu autonomicznego routera wysyłającego komunikat i numerze porządkowym komunikatu. Dodatkowo w nagłówku jest zawarta suma kontrolna używana do zabezpieczenia danych (protokół EGP używa do przesyłania swoich komunikatów datagramów IP; wiadomo, że protokół IP zabezpiecza tylko nagłówek datagramu IP). Warto zwrócić też uwagę na fakt, że komunikat GGP nie stosował specjalnych zabezpieczeń przed błędami, a jedynym użytym w nim mechanizmem zabezpieczającym było potwierdzanie komunikatów o zmianie tras.

Protokół EGP realizuje 3 podstawowe funkcje:

- **pozyskiwanie sąsiada** - Router wysyła komunikat typu „neighbour acquisition”, by nawiązać połączenie z innym routерem, w celu wymiany informacji o dostępnych trasach. W protokole EGP nie jest określone, jak router wybiera sąsiada. Zakłada się, że ustala to organizacja administrująca routera. Komunikat pozyskiwania sąsiada definiuje też wartość przedziału czasu między komunikatami testującymi połączenie z sąsiadem oraz odstęp czasu między zapytaniami o aktualizację tras.
- **sprawdzanie osiągalności sąsiada** - Router realizujący EGP sprawdza (monitoruje), czy sąsiad jest „aktywny”, przy czym może to robić na dwa sposoby. W trybie aktywnym router okresowo wysyła komunikaty z zapytaniami *Hello* i czeka na komunikaty odpowiadające na te zapytania. W trybie biernym router odpowiada tylko na zapytania sąsiada. Normalnie jednak oba routery stanowiące parę pracują w trybie aktywnym. Oddzielenie komunikatu o osiągalności od komunikatu z informacjami o trasach redukuje ruch w sieci, ponieważ informacje o trasach nie zmieniają się tak często, jak zmieniają się stany poszczególnych routerów. Komunikaty *Hello* mogą zaginąć. By stwierdzić, że partner nie działa, protokół EGP stosuje tzw. regułę „*k spośród n*”. Oznacza to, że przynajmniej k spośród n ostatnich wymian komunikatów *Hello* musi zawiść, by stwierdzić brak sąsiada. Odwrotnie, co najmniej j wymian musi zajść poprawnie, aby zerwane połączenie zostało przywrócone. Zastosowana tu „histereza” powoduje, że EGP nie propaguje tras不稳定nych.
- **przesyłanie informacji o osiągalności** - Routery wysyłają komunikaty z informacjami o osiągalności sieci wewnętrznych ich systemów autonomicznych. Routery mogą pytać sąsiadów o informacje o osiągalności poprzez wysyłanie komunikatu EGP z „prośbą o dane”. Komunikat taki zawiera, poza standardowym nagłówkiem, tylko pole z adresem IP sieci początkowej, określającym, jaka sieć ma być użyta jako punkt odniesienia. Drugi router danej pary wysyła komunikat-odpowiedź. Komuni-

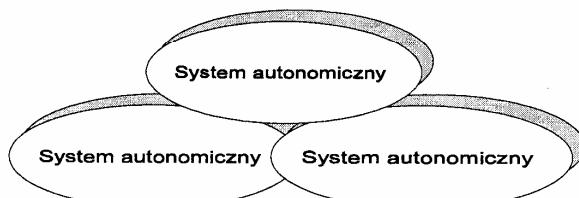
kat ten zawiera informacje o tym, ile routerów wewnętrznych i ile zewnętrznych występuje w komunikacie oraz podaje adres sieci początkowej (określający sieć, względem której wyznaczono odległości poszczególnych sieci (celów) zawartych w komunikacie). W komunikacie znajduje się również zbiór bloków, z których każdy zawiera adres IP routera i adresy sieci osiągalnych przez ten router, wraz z ich odległościami od sieci początkowej. Podobnie jak w GGP, wewnątrz każdego bloku trasy są pogrupowane według odległości.

EGP nie interpretuje odległości zawartych w komunikacjach i nie próbuje wybrać najlepszej ścieżki. EGP aktualnia jedynie informacje dystansowo-wektorowe, lecz bez ich przetwarzania. Pochodzą one bowiem z różnych systemów autonomicznych SA, z których każdy może stosować inne kryteria do tworzenia tras (w przypadku tego samego SA można dokonać takiego porównania). Z tego powodu EGP pozostawia sprawę wyboru ścieżki innemu protokołowi. EGP podaje odległość tylko po to, by można było stwierdzić, że dana sieć istnieje wewnątrz systemu autonomicznego. Dlatego też EGP można trafić określić mianem protokołu osiągalności sieci, niż protokołu routingu. Protokół EGP jest w dalszym ciągu często stosowanym algorytmem wymiany informacji, pozwalającym na ocenę dostępności sieci. Specyfikację EGP można znaleźć w RFC 904.

#### Rozprosiona struktura routingu

Hierarchiczna struktura routingu, która była używana w początkowej fazie rozwoju Internetu, miała jedną podstawową wadę - każdy pakiet przesyłany między różnymi SA musiał przejść przez jądro. Powodowało to, wraz z rozwojem Internetu, ogromne obciążenie jądra, szczególnie routerów jądra, które musiały przetwarzać informacje o trasach z całego Internetu. Był to jeden z powodów, dla których wprowadzono rozproszoną metodę przetwarzania informacji routinguowej.

Nowy rozproszony model routingu (patrz rysunek 9.37) wykorzystuje zbiór równoprawnych systemów autonomicznych, zwanych domenami routingu.



Rys. 9.37. Rozprosiona struktura organizacji pracy sieci i algorytmów routingu

Systemy autonomiczne wymieniają informacje o trasach, używając jednego z zewnętrznych protokołów routingu. Coraz popularniejszym protokołem tego typu staje się obecnie BGP (ang. *Border Gateway Protocol*). Ciągle jednak istnieje moż-

liwościość użycia protokołu EGP. Ze względu na ograniczenie nakładane przez ten protokół na topologię sieci (musi to być struktura drzewiasta z jądrem jako korzeniem) jest on coraz bardziej wypierany przez inne protokoły, w tym BGP. Każdy system autonomiczny przetwarza, wg własnych potrzeb, informacje otrzymane z innych systemów autonomicznych. Wewnątrz systemów autonomicznych używane są przy tym, zgodne z BGP, wewnętrzne protokoły routingu (IGP).

#### Border Gateway Protocol

*Border Gateway Protocol* (BGP) opracowany specjalnie jako zewnętrzny protokół routingu między domenami (systemami autonomicznymi) jest próbą rozwiązania problemów EGP. Obecnie używana jest 4 wersja tego protokołu.

Odmiennie od wcześniej omawianych protokołów BGP korzysta, do wymiany informacji między routerami, z protokołu TCP. Upraszczając to znacznie graf stanów protokołu. TCP gwarantuje bowiem poprawność i integralność przesyłanych danych. Użycie TCP pozwala zmniejszyć obciążenie sieci, poprzez przesyłanie w sposób niezawodny tylko informacji o zmianach tras, w przeciwieństwie do tradycyjnego rozwiązania, stosowanego w EGP, zgodnie z którym przesyłano całe tablice tras. Ażkolwiek BGP został zaprojektowany jako zewnętrzny protokół routingu, może on być również używany jako protokół wewnętrzny (w ramach danego systemu autonomicznego). Podobnie jak w EGP dwa komunikujące się ze sobą routery nazywane są sąsiadami. Definiowani są przy tym sąsiedzi zewnętrzni, tj. należący do różnych systemów autonomicznych oraz sąsiedzi wewnętrzni, należący do tego samego SA. Sąsiedzi wewnętrzni komunikują się między sobą w celu ustalenia jednolitej oceny stanu systemu autonomicznego oraz określenia, który z routerów BGP będzie służył jak punkt połączenia do i z poszczególnymi systemami autonomicznymi.

Informacje o trasach, przesyłane przez BGP, zawierają pary liczb (adres sieci, ścieżka SA), gdzie ścieżka SA jest łańcuchem systemów autonomicznych, przez które należy przejść, by dotrzeć do określonej sieci. Początkowo, między dwoma routerami przesyłane są całe tablice routingu; później przesyłane są jedynie informacje o zmianach w tablicach routingu. Możemy więc mówić o wymianie informacji w trybie przyrostowym. BGP nie wymaga też periodycznego przesyłania aktualizowanych danych routingu. Protokół BGP przechowuje tablice routingu wraz ze wszystkimi możliwymi ścieżkami, jednakże rozmawia innym routerom tylko ścieżki optymalne.

Każdy komunikat BGP ma określony standardowy nagłówek i dodatkowe pola zależne od typu komunikatu. BGP definiuje cztery typy komunikatów:

- Komunikat *Open* - Jest on pierwszym komunikatem wysyłanym przez router. Służy on do nawiązania połączenia i pozyskania sąsiada. Jeśli komunikat *Open* zostanie zaakceptowany, to druga strona przesyła jako potwierdzenie - komunikat *Keepalive*. Komunikat *Open* zawiera między innymi pola określające wersję protokołu BGP i numer systemu

autonomicznego nadawcy. Oprócz tego w komunikacie zawarty jest też kod autentyfikacji, mówiący o użytym typie autentyfikacji oraz pole *hold-time* wyznaczające maksymalny czas, jaki może upłynąć bez odebrania komunikatu od sąsiada, zanim zostanie on uznany za sąsiada nieaktywnego.

- Komunikat ***Update*** - Komunikat ten zawiera informacje o trasach (jeśli jest to początek komunikacji) lub zawiera tylko informacje o zmianach tras (po nawiązaniu komunikacji). Router wykorzystuje te informacje do stworzenia mapy połączeń systemów autonomicznych. Oprócz standardowego nagłówka występują w nim dodatkowe pola, które rozszerzają informację o trasach przez podanie atrybutów ścieżek dla każdej z sieci. Podstawowe atrybuty to:

*Origin* - określa on pochodzenie informacji o trasie. Źródłem może być wewnętrzny protokół routingu (IGP), zewnętrzny protokół routingu (EGP) lub też informacja może mieć całkiem inne pochodenie.

*AS path* - podaje on aktualną listę systemów autonomicznych, przez które przechodzi trasa do określonej w komunikacie sieci. Umożliwia to wykrywanie pętli.

*Next hop* - parametr ten określa adres IP routera, który jest następnym etapem na podanej ścieżce określonej przez *AS path*.

*Unreachable* - atrybut ten oznacza (o ile występuje), że trasa nie jest już aktualna.

*Inter-AS metric* - zawiera on informacje o koszcie trasy do sieci przeznaczenia, wewnątrz danego systemu autonomicznego. Pozwala to zewnętrznym routerom na wyznaczenie optymalnej trasy przebiegającej przez dany system autonomiczny.

- Komunikat ***Notification*** - W przypadku wystąpienia błędów i podjęcia przez router decyzji o przerwaniu połączenia, wysyłany jest komunikat *Notification*. Oprócz normalnego nagłówka BGP zawiera on typ błędu, podtyp błędu oraz informacje dodatkowe dotyczące błędu.
- Komunikat ***Keepalive*** - Komunikaty *Keepalive* nie zawierają żadnych dodatkowych pól oprócz standardowych pól nagłówka i służą do podtrzymania połączenia między komunikującymi się routerami. Częstość wysyłania komunikatów określa pole *hold-time* w komunikacie *Open*.

Atrybuty ścieżek mogą też zawierać informacje służące do wyboru tras na podstawie preferencji administracyjnych. Są one zwykle ustawiane przez administratora sieci poprzez pliki konfiguracyjne. BGP umożliwia realizację określonej strategii routingu, tzn. pozwala na wyznaczanie tras nie tylko ze względu na przesłanki techniczne, ale też ze względów innego rodzaju, np. politycznych, bezpieczeństwa, itp. Bardzo ważną cechą protokołu BGP, w wersji czwartej, jest umożliwienie łączenia adresów, wymagane przez routing bezklasowy (CIDR).

BGP jest obecnie najpopularniejszym zewnętrznym protokołem routingu. Został on jednakże zaprojektowany do obsługi adresów 32 bitowych. Z tego powodu wydaje się on być mniej przydatny dla następnej generacji protokołów Internet (IPv6), dla której przewidziano adresy 128 bitowe. IETF, przyjęła, że podstawowym protokołem routingu zewnętrznego dla IP wersji 6 będzie protokół, skrótnie oznaczany jako IDR (ang. *Inter-Domain Routing Protocol*). Najnowsza wersja BGP opisana jest w RFC 1771.

#### Wewnętrzne protokoły routingu

Wewnętrzne protokoły routingu służą do wyznaczania tras wewnątrz systemu autonomicznego. Wybór protokołu dokonywany jest przez organizację zajmującą się administracją danego SA. Istnieje wiele wewnętrznych protokołów routingu (ang. IGP - *Interior Gateway Protocol*). Najbardziej znane to RIP, OSPF, Hello, IS-IS i EIGRP.

#### Routing Information Protocol

Protokół RIP był protokołem bardzo popularnym w początkowej fazie rozwoju Internetu. Jego popularność wynikała zarówno z prostoty rozwiązania jak też z faktu, że oprogramowanie tego protokołu (program *routed*) był częścią składową większości systemów UNIX. RIP, zaprojektowany przez firmę Xerox, jest typowym przykładem protokołu wektorowo-odległościowego. Jako trasy najlepsze wybiera on trasy charakteryzujące się najmniejszą liczbą etapów transmisji (skoków - ang. *hops count*), związane jednocześnie z najmniejszą liczbą routerów, przez które musi przejść datagram, by trafić do adresata.

RIP dzieli dołączone do sieci urządzenia na czynne i bierne. Urządzenia czynne oferują innym swoje informacje o trasach, bierne zaś mogą wyłącznie modyfikować swoje tablice routingu. Normalnie tylko router może używać protokołu RIP w trybie czynnym, zwykłe komputery pracują normalnie w trybie biernym.

Routery realizujące RIP rozmawiają co 30 sekund komunikaty zawierające aktualne informacje o trasach. Każdy komunikat zawiera pary liczb określające adres IP sieci i odległość (tzn. liczbę etapów) do tej sieci od danego routera. Według protokołu RIP router znajduje się w odległości jednego etapu od sieci, jeśli jest bezpośrednio do niej połączony, w odległości dwóch etapów, jeśli sieć jest osiągalna za pomocą jednego routera, itd. Każde urządzenie, które używa protokołu RIP, odbiera rozmawiane komunikaty i na ich podstawie modyfikuje swoją tablicę routingu. Sprawdza przy tym czy router, który wysłał komunikat, zapewnia połączenie do jakiejś sieci z mniejszą liczbą etapów niż to wynika z zapisu w jego własnej tablicy routingu (uwzględnia przy tym to, że do wszystkich odległości w otrzymanym komunikacie należy dodać 1, przed dokonaniem porównania). Jeśli otrzymana w wyniku tego porównania wartość jest mniejsza, to zostaje ona umieszczona w tablicy. W praktyce oznacza to, że dana sieć jest osiągalna poprzez router nadający komunikat (adres routera zostaje zapisany w polu *next hop*). Jeśli

router odbierający nie ma jeszcze w swojej tablicy jakieś sieci, wymienionej w komunikacie, to także wpisuje jej adres do tablicy routingu z liczbą etapów zwiększoną o 1 i adresem routera rozgłaszającego komunikat jako *next hop*. Z każdą pozycją w tablicy routingu jest związany licznik czasu (timer), który jest uruchamiany po każdorazowym otrzymaniu komunikatu RIP, oferującego tę trasę. Trasa jest usuwana, jeśli w określonym czasie (typowo 90 s lub 180 s) nie zostanie ponownie zaoferowana.

RIP jest protokołem prostym i łatwym w implementacji, niepozbawionym jednak szeregu wad. Jedną z nich jest powolna stabilizacja tras po wystąpieniu zmian. Może to powodować powstawanie tymczasowych pętli. RIP nie wykrywa także automatycznie pętli w trasach.

RIP korzysta z prostego algorytmu wyznaczania tras opartego na metryce odległości i nie uwzględnia innych bardzo ważnych parametrów, takich jak np. przepustowość łącz, jakość transmisji, koszty połączeń, itp.

RIP nakłada ograniczenie na maksymalną liczbę etapów transmisji. Najdłuższa trasa jaką akceptuje może się składać z 16 etapów. Ograniczenie to, wynikające z powolnej zbieżności algorytmu, pozwala zmniejszyć skutki tego faktu. RIP wysyła co 30 sekund komunikaty zawierające całe tablice routingu. Przy dużych sieciach może to spowodować, że znaczną część ruchu w sieci będzie związana z informacjami routingowymi.

W swojej podstawowej wersji RIP nie zapewnia też uwierzytelniania komunikatów. Pozwala to komuś niepowołanemu na przesyłanie komunikatów routingowych i tym samym zakłócanie całego procesu ustalania optymalnych tras. Problem ten rozwiązano w drugiej wersji RIP (RIPv2) będącej rozszerzeniem podstawowej wersji protokołu RIP (oznaczanego RIPv1).

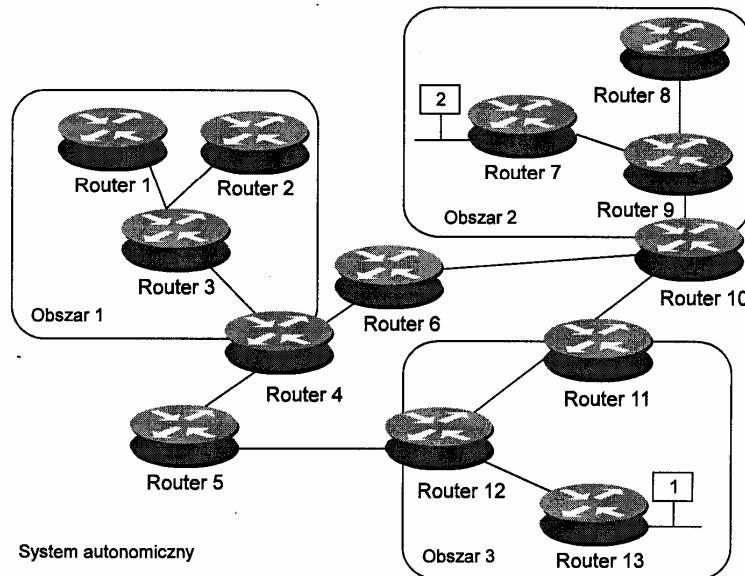
Jedną z dodatkowych możliwości RIPv2 jest właśnie uwierzytelnianie komunikatów RIP. RIPv2 może to robić na dwa sposoby. Pierwszy polega na przesyłaniu w komunikacie prostego 16 znakowego hasła. Jeśli przesłane hasło nie będzie się zgadzać z oczekiwany, to komunikat zostanie odrzucony. W drugiej metodzie wykorzystywany jest algorytm MD5 służący do wyliczenia kryptograficznej sumy kontrolnej. Transmitowany komunikat nie zawiera przy tym klucza uwierzytelniającego, a jedynie sumę kontrolną. Odbiorca komunikatu zna klucz uwierzytelniający i przy jego pomocy wylicza kryptograficzną sumę kontrolną, a następnie porównuje wynik własnych obliczeń z sumą odebraną. Jeśli obie sumy nie są identyczne, to komunikat jest odrzucony. W celu zabezpieczenia przed ponownym wysłaniem starego komunikatu, wprowadza się numery porządkowe.

RIPv1 przyjmuje, że wszystkie podsieci, w ramach jednej sieci, mają taką samą maskę. Jeśli wystąpią podsieci o różnych długościach masek, to tylko podsieci z jedną i tą samą maską zostaną uwzględniane w komunikatach RIPv1. Wszystkie podsieci mające inne maski będą pominięte. RIPv2 daje możliwość dokładnego określenia maski dla każdej podsieci.

#### Open Shortest Path First

OSPF jest protokołem routingu wewnętrznego (IGP) opracowanym z myślą o współpracy z protokołem IP. Opis protokołu OSPF w jego wersji 2 (obecnie używanej) znajduje się w RFC 1583. Jak wskazuje pierwsza część nazwy protokołu (*Open* - ang. otwarty), OSPF jest otwarty, a jego specyfikacja jest ogólnie dostępna. Druga część nazwy wskazuje, że wykorzystuje on algorytm SPF (ang. *Shortest Path First*), tzn. algorytm stanu łączka pozwalający na wybór ścieżki najkrótszej.

OSPF umożliwia routing zależny od typu usługi. Oznacza to, że zalecana trasa może być zależna od podanego w nagłówku IP typu obsługi. Ważną zaletą OSPF jest to, iż zapewnia on równoważenie obciążenia, tzn. dzielenie ruchu między kilka tras o jednakowym koszcie. OSPF wymaga też uwierzytelniania informacji przesyłanej między routerami. OSPF wykorzystuje przy tym dwa rodzaje uwierzytelniania, bardzo podobne do oferowanych przez RIPv2.



Rys. 9.38. Hierarchiczna struktura routingu OSPF

OSPF jest protokołem routingu wewnętrznego, używanym wewnętrznie systemu autonomicznego, będącego zbiorem wspólnie administrowanych sieci. OSPF umożliwia jednakże dalszy podział hierarchiczny architektury routingu. Daje on możliwość podziału systemu autonomicznego na obszary. Obszar jest to zbiór połączonych sieci oraz przyłączonych do nich komputerów i routerów. Router z wieloma interfejsami może należeć do wielu obszarów. Nazywany jest wtedy routерem brze-

gowym (ang. *area border router*). Routery tego typu utrzymują osobne bazy danych o topologii każdego z obszarów. Każda baza danych topologii jest mapą opisującą sieć, w postaci grafu połączeń między routerami. Routery tworzą te bazy na podstawie otrzymanych komunikatów o zmianie stanu łączy (typu *link-state advertisement*), od wszystkich routerów danego obszaru. Komunikat *link-state advertisement* zawiera informacje o stanie połączeń, od routera nadającego do wszystkich jego sąsiadów. Wszystkie routery w danym obszarze otrzymują te same informacje, dlatego też wszystkie one mają te same mapy obszaru. Topologia obszaru nie jest jednak widoczna poza nim. Ograniczanie tworzenia mapy sieci tylko do rozmiaru pojedynczego obszaru pozwala na zmniejszenie ruchu sieciowego związanego z wymianą informacji o trasach, w porównaniu z przypadkiem nie dzielenia systemu autonomicznego na mniejsze obszary. OSPF definiuje „szkielet”, który jest odpowiedzialny za przekazywanie informacji routingowej między obszarami. Do szkieletu tego należą: routery brzegowe obszarów, sieci nie należące w całości do któregoś z obszarów i przyłączone do nich routery. Rysunek 9.38 pokazuje przykładowy system autonomiczny ze szkieletem i trzema obszarami. Na rysunku tym routery 4, 5, 6, 10, 11 i 12 tworzą wspomniany wyżej szkielet. Sam szkielet też jest obszarem i dlatego jest w nim używany ten sam algorytm do tworzenia map szkieletu, jak w innych obszarach. Topologia szkieletu nie jest widoczna dla routerów, które zajmują się routingiem jedynie wewnątrz swojego obszaru (tzw. *intra-area router*). Podobnie też topologia poszczególnych obszarów nie jest widoczna dla szkieletu.

Obszary mogą być też zdefiniowane tak, że szkielet będzie nieciągły. W przypadku braku ciągłości, połączenia muszą być utrzymane przez połączenia wirtualne (ang. *virtual link*). Wirtualne połączenia są zestawiane pomiędzy routerami należącymi do szkieletu, nie mającymi jednak bezpośredniego połączenia.

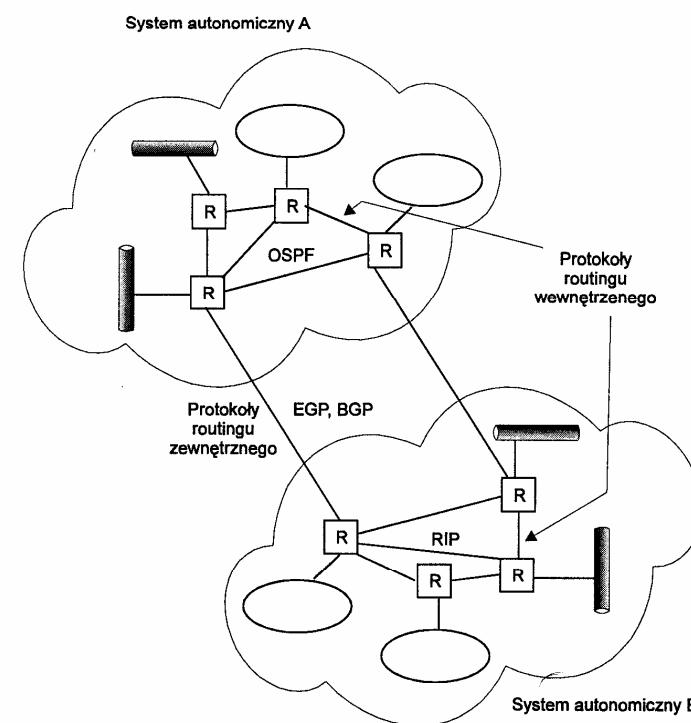
OSPF zawiera w sobie trzy protokoły (w przeciwieństwie do protokołu RIP, w którym funkcjonował tylko jeden protokół). Najważniejsze z nich to OSPF Hello protocol i protokół wymiany baz danych.

**OSPF Hello protocol** - Protokół ten jest używany przy inicjalizacji pracy routera do pozyskania jego sąsiada. Sąsiadami, wg. OSPF, są routery przyłączone do tej samej sieci. Router wysyła komunikaty *hello* do sąsiadów i odbiera od nich komunikaty *hello* jako odpowiedzi. Po nawiązaniu komunikacji sąsiedzi przesyłają komunikaty *hello* co pewien określony czas, aby upewnić się, czy druga strona nadal funkcjonuje. W sieciach, do których podłączone są więcej niż dwa routery, protokół *Hello* wybiera, dodatkowo, wyróżniony router (ang. *destinated router*) oraz zastępczy wyróżniony router (ang. *backup destinated router*). Jedną z funkcji wyróżnionego routera jest generowanie komunikatów *link-state advertisement* dla sieci z wieloma przyłączonymi routerami. Pozwala to zmniejszyć ruch w sieci i rozmiary baz danych topologii. Wyróżniony router określa też, w takich sieciach, jakie routery mają się komunikować ze sobą w celu wymiany informacji.

**Protokół wymiany baz danych** - Routery z najbliższego sąsiedztwa, które zostały wyznaczone do wzajemnej komunikacji przez router wyróżniony (po angielsku określa się je jako *adjacent*), przesyłają między sobą komunikaty *Database description*, które zawierają bazę danych z topologią sieci. Komunikaty te nie są przesyłane między wszystkimi sąsiadami, by nie powodować niepotrzebnego przepływu informacji.

Każdy router, który wykryje zmianę stanu któregoś ze swoich łączy z sąsiadem (np. zerwanie wymiany komunikatów *hello*), rozsyła, do wszystkich pozostałych routerów w obszarze, komunikaty *link-state advertisement*.

OSPF jest zalecanym wewnętrzny protokół routingu dla IPv6. W związku z tym IETF tworzy wersję OSPF dla IPv6. Oczekuje się, że zmiany w protokole będą niewielkie, mające jedynie na celu przystosowanie do większych rozmiarów adresów. Ilustrację wykorzystania protokołów wewnętrznych i zewnętrznych w połączonych systemach autonomicznych stanowi rysunek 9.39.



Rys. 9.39. Przykładowe protokoły routingu wewnętrzne i zewnętrzne

#### 9.3.4.4 Routery w sieciach Novell

Jednym z najbardziej popularnych oprogramowań sieciowych stosowanych w środowisku sieci LAN jest sieciowy system operacyjny Novell NetWare.

Oprogramowanie NetWare instalowane w stacjach roboczych i serwerach pozwala przede wszystkim na współpracę stacji DOS-owych, OS/2-owych i Macintosh-owych. Sieciowy system operacyjny NetWare obejmuje:

- tzw. powłokę NetWare (ang. *NetWare Shell*), stanowiącą Program Nadzorujący Pracę Sieci (ang. *Network Control Program*) oraz emulator popularnego interfejsu sieciowego NETBIOS, czyli protokoły pozwalające na współpracę z systemem operacyjnym DOS i aplikacjami DOS-owymi,
- protokoły wymiany pakietów IPX/SPX (ang. *Internetwork Packet Exchange / Sequenced Packet EXchange*) - wzorowane na protokołach architektury XNS - zapewniające komunikację z pozostałymi komputerami sieci (stacjami roboczymi i serwerami) i stanowiące interfejs pomiędzy aplikacjami a podsiecią komunikacyjną,
- moduł kontrolera (ang. NIM - *Network Interface Modul*) gwarantujący współpracę z np. sieciami Ethernet, Token Ring, ARCnet, FDDI.

Podstawowym protokołem komunikacyjnym w sieciach Novell jest protokół datagramowy IPX. Pakiet IPX wyposażony jest w szereg pól, w tym 12-sto bajtowe pola z adresami stacji docelowej i źródłowej. Adres sieciowy składa się z trzech elementów:

- adresu sieci (4 bajty),
- adresu stacji, będącej jej adresem fizycznym (6 bajtów), oraz
- identyfikatora procesu aplikacyjnego (2 bajty).

Protokół dopuszcza transmisję pakietu przez maksymalnie 16 routerów.

Funkcje routingu implementowane są w routerach. Definiowane są przy tym tzw. routery wewnętrzne i zewnętrzne. W pierwszym przypadku router może pełnić jednocześnie i inne funkcje, np. serwera zbiorów bądź też bramy pomiędzy siecią Novell i SNA. Router zewnętrzny jest prostą stacją roboczą wyposażoną zwykle w kilka kart sieciowych i realizującą wyłącznie funkcje routingu.

Routery Novell-a konstruują tablice z kompletną informacją o wszystkich innych aktywnych routerach IPX i sieciach, w ramach danego internetu. Tablice zawierają adresy poszczególnych sieci, liczby routerów tranzytowych, ocenę czasu transmisji (określaną na podstawie szybkości transmisji w poszczególnych segmentach sieci LAN), numery kart sieciowych związanych z odpowiednimi portami danego routera, numery fizyczne routerów sąsiednich, status poszczególnych sieci, czasy ostatniego aktualizowania informacji routingu (max. 60 sekund).

Routery IPX wymieniają zawartości tablic korzystając przy tym z protokołu RIP. Protokół wymiany informacji routingu RIP jest algorytmem powszechnie stosowanym we współczesnych sieciach komputerowych. Modyfikacje tego proto-

ku są stosowane w sieciach TCP/IP, AppleTalk, XNS. Podstawowym zadaniem protokołu jest dostarczanie użytkownikowi informacji o „najszyszej” trasie przekazu informacji, w odpowiedzi na żądanie trasy zgłoszone w postaci zgłoszenia.

#### 9.3.4.5 Koncepcja routingu w modelu ISO-OSI

Problematyka łączenia sieci w celu uzyskania jednorodnego „internetu” jest przedmiotem wielu prac standaryzacyjnych ISO. W kręgu zainteresowań ISO znajdują się sieci oferujące zarówno usługi połączeniowe jak i bezpołączeniowe. W przypadku sieci z obsługą połączeniową wykorzystywany jest głównie protokół pakietowy PLP (ang. *Packet Layer Protocol*) warstwy sieciowej stanowiący element standardu X.25. Protokół PLP pozwala też na współpracę z sieciami ISDN. Specyfikacja ISO 8348, regulująca usługi bezpołączeniowe, poza opisem sposobu implementacji tych usług, zawiera też uniwersalny schemat adresacji, dostosowany do szeregu wcześniej opracowanych metod.

##### 9.3.4.5.1 Zasady adresacji ISO

Jednym z podstawowych problemów wymagających jednoznacznego zdefiniowania w przypadku przekazu informacji pomiędzy podsieciami komputerowymi, tworzącymi strukturę internetu, jest zagadnienie adresów sieciowych. W przypadku sieci realizujących protokoły ISO-OSI implementowany jest standard adresowy ISO. Zgodnie z nim adresy sieciowe mogą mieć zmienną długość nie przekraczającą jednakże 20 bajtów; jeden z bajtów wskazuje przy tym długość całego adresu. Adres ISO składa się z trzech zasadniczych pól:

- pola definiującego adres podsieci pierwszego poziomu, bądź adres sieci poszczególnych poziomów,
- pole identyfikatora ID stacji końcowej,
- pola SEL specyfikującego protokół warstwy transportowej korzystający z usługi sieciowej.

W przypadku adresów objętych specyfikacją ISO 8348 pełny adres stacji w sieci LAN dołączonej do internetu OSI ma więc postać:

Adres = <adres podsieci> <adres MAC> <LSAP> <NSAP>

Adres podsieci jest zwykle poprzedzony identyfikatorem organizacji ustalającej składnię i semantykę adresu, tutaj - ISO.

Identyfikator ID stacji końcowej obejmuje adres fizyczny stacji (adres MAC karty sieciowej) i adres punktu LSAP. Z kolei pole SEL definiuje protokół transportowy i stanowi adres NSAP.

Wartości LSAP i NSAP określają protokoły warstw: sieciowej i transportowej zaangażowane do realizacji usług internetowych. W przypadku protokołu siecio-

wego IP OSI wartość LSAP będzie zawsze równa Hex FE, natomiast protokół OSI-TP4 będzie związany z wartością selektora NSAP równą 1.

Zgodnie z koncepcją współpracy warstwowej Modelu ISO-OSI, właściwy przepływ informacji wewnątrz stacji końcowej z warstwy transportowej do warstwy aplikacji i z powrotem wymaga oczywiście przydziału dodatkowych selektorów SAP (TSAT, SSAP i PSAP) będących zwykle dwubajtowymi ciągami binarnymi.

W przypadku realizacji routingu hierarchicznego, router pierwszego poziomu dokonuje porównanie adresu docelowego pakietu z jego własnym adresem. Jeżeli porównywane adresy są identyczne, wówczas router kieruje pakiet zgodnie zasadą routingu obowiązującą w danej podsieci. W przypadku niezgodności adresów kieruje on dany pakiet do najbliższego routera drugiego poziomu. Routing na tym poziomie (i poziomach wyższych) dokonywany jest z wykorzystaniem właściwego przedrostka adresu sieciowego.

### 9.3.4.5.2 Protokół IP OSI

Koncepcja realizacji bezpołączeniowych, tj. datagramowych usług w internecie ISO-OSI, jest próbą uelastycznienia pracy sieci implementujących tę architekturę. Internetowy protokół OSI (OSI IP) jest funkcjonalnie równoważny protokołowi IP z architektury TCP/IP, oferując kilka dodatkowych możliwości. Podstawowe funkcje i parametry obu protokołów pozostają przy tym identyczne. W szczególności oba protokoły uwalniają stacje końcowe od konieczności przechowywania informacji o:

- routingu w internecie,
- maksymalnych rozmiarach pakietów w poszczególnych podsieciach internetu,
- jakości usług oferowanych przez połączone sieci.

OSI IP realizuje powyższe zagadnienia:

- zapewniając dynamiczny i alternatywny routing,
- dokonując segmentacji/resegmentacji przesyłanych datagramów,
- uwzględniając jakość świadczonych usług przy podejmowaniu decyzji o wyborze trasy.

Podstawowa jednostka danych, określana mianem IPDU (*Internet Protocol Data Unit*) składa się z pięciu podstawowych bloków. Są to:

- stała część IPDU definiująca między innymi wersję protokołu IP, podającą czas życia pakietu, informacje na temat ewentualnej segmentacji oraz obejmująca ciąg kontrolny,
- część adresowa IPDU, zawierająca adresy stacji źródłowej i docelowej wraz z adresami punktów dostępu do usług (NPSA), identyfikującymi protokoły warstwy transportowej,
- część organizacyjną IPDU związaną z segmentacją bloku danych (o ile segmentacja jest wymagana),

- część opcjonalną definiującą pożądane parametry obsługi datagramu,
- blok danych.

### 9.3.4.5.3 IP-OSI routing

Protokół IP-OSI opisuje zasady komunikowania się systemów pośredniczących (ang. *Intermediate Systems - IS*) czyli routerów sieci i/lub systemów końcowych (ang. *End Systems - ES*), stanowiących, zgodnie z terminologią ISO, komputery dołączone do sieci.

Protokół współpracy ES-IS definiuje zalecenie ISO 9542. Z kolei zasady współpracy pomiędzy routerami, czyli systemami pośredniczącymi IS-IS, opisuje standard ISO 10589. Oba dokumenty specyfikują protokoły routingu dla sieci bezpołączniowych.

Internet OSI powinien oferować dynamiczny i w pełni rozproszony routing szybko reagujący na wszelkie zmiany w topologii sieci.

Cel ten można osiągnąć stosując dwie strategie routingu:

- proste i popularne rozwiązanie z protokolami dystansowo-wektorowymi (ang. *Distance Vector Approach Protocol*) polegające na zapamiętywaniu w routerach sieci tablic z podanymi liczbami etapów transmisji z danego routera do innych routerów sieci,
- rozwiązanie wykorzystujące informacje o stanach łączy w sieci (ang. *Link State Protocol*), nazwane też algorytmem najkrótszych ścieżek, z uwagi na selekcję dróg połączeniowych w oparciu o najmniejszą wartość przyjętej metryki. Metrykę łącza może przy tym stanowić opóźnienie, koszt transmisji, prawdopodobieństwo błędu, itp. Każdy router (IS) konstruuje własną bazę danych - tablicę routingu.

Sieci typu globalnego internetu są ze względów praktycznych dzielone na podsieci, tworząc obszary, domeny, grupy domen i ostatecznie - sieć globalną. W internecie OSI definiuje się czteropoziomową hierarchię routingu. Poszczególne "poziomy" w tej hierarchii mają swoje routery odpowiedzialne za wybór tras w danym obszarze oraz ewentualnie - przekaz informacji z danego poziomu na poziom wyższy. Taka organizacja pozwala utrzymywać w węzłach tablice wyboru tras o ograniczonych wymianach, chroniąc całą sieć przed nieprawidłowościami pracy w określonej podsieci oraz pozwala na wybór zasad routingu dostosowanych do potrzeb i wymagań sieci lokalnej.

Na każdym poziomie realizacji routingu protokół OSI IP posiada opcjonalne mechanizmy pozwalające na usuwanie datagramów z sieci w przypadku wystąpienia stanu silnego przeciążenia. Jest to cecha charakteryzująca wiele protokołów bezpołączniowych, rzutująca na ich zawodny charakter, objawiający się dodatkowo brakiem sterowania przepływem pakietów i brakiem gwarancji dostarczania datagramów do adresata w ustalonej kolejności.

W przypadku OSI-IP zarówno systemy (stacje) końcowe ES jak i routery (IS) mają możliwość przesyłania specjalnych pakietów "hello", nadawanych w trybie rozgłoszeniowym i powiadamiającym węzły sąsiednie o obecności stacji ES bądź IS w sieci. Pozwala to na aktualnienie poszczególnych wejść w tablicach wyboru tras. Brak informacji "hello" przy jednoczesnym braku aktywności stacji/węzła przez określony czas powoduje usunięcie stosownej informacji routingowej z ablicy.

### 9.3.5 Bramy/konwertery protokołów

Brama to wspólna nazwa dla szeregu urządzeń realizujących konwersję formatów danych między różnymi protokołami. W przypadku dołączania do sieci o zadanej architekturze logicznej innych sieci komputerowych, ich protokoły muszą podlegać stosownej konwersji, w celu zapewnienia zgodności ze standardami obowiązującymi w sieci podstawowej i umożliwienia tym samym komunikacji między urządzeniami końcowymi. W odróżnieniu od omawianych poprzednio urządzeń (mosty, routery) bramy nie zawsze separamają różne sieci fizyczne. Bramy pracują na poziomach warstw: transportowej, sesji, prezentacji i aplikacji (patrz rysunek 9.6). Jako przykład takiego urządzenia można podać bramę realizującą konwersję protokołu poczty w standardzie X.400 na standard SMTP. Bramy są najczęściej specjalizowanym oprogramowaniem zainstalowanym na stacjach roboczych bądź komputerach obliczeniowych.

Bramy są urządzeniami projektowanymi głównie dla połączeń między sieciami o odmiennych architekturach. Pełnią one funkcje konwerterów protokołów poszczególnych warstw w obu łączonych architekturach. Często przyjmuje się, że podstawową cechą bramy jest konwersja protokołów, niezależnie od ich lokalizacji w architekturze warstwowej. Zgodnie z taką definicją połączenie dwóch sieci LAN o odmiennych protokołach warstwy łącza danych, np. sieci Token Ring i sieci Ethernet, wymagające konwersji protokołów podwarstwy MAC i ewentualnie LLC, dokonywane będzie za pośrednictwem bramy warstwy drugiej Ethernet/Token Ring. Bramę taką nazywać jednakże będziemy konsekwentnie mostem – przyjmując jako podstawę takiej kwalifikacji fakt dokonywania przekształceń protokolarnych w warstwie drugiej modelu ISO/OSI.

W przypadku łączenia sieci SNA i DECnet bądź OSI zachodzi konieczność translacji protokołów wszystkich warstw, z protokołem warstwy aplikacji włącznie.

W zależności od typów łączonych ze sobą sieci, definiujemy różne typy bram:

Bramy OSI / TCP/IP pozwalają sieciom OSI i TCP/IP na współpracę, dokonując np. konwersji protokołu transportowego TP4 (klasy czwartej OSI) na TCP.

Z kolei bramy oferowane przez DEC do współpracy z siecią SNA, tj. bramy DECnet/SNA, dokonują przekształcenia protokołów aplikacyjnych sieci DECnet do postaci protokołów stosowanych np. w terminalach IBM serii 3270. Emulacja

funkcji IBM 3270 pozwala na dostęp użytkowników sieci DECnet do zasobów (programów aplikacyjnych) komputerów głównych sieci IBM.

Bramy TCP/IP / SNA pozwalają na interaktywne komunikowanie się aplikacji w obu sieciach, czyli np. na współpracę UNIX-owych stacji sieci TCP/IP i komputerów MVS sieci SNA. Dokonują one konwersji wywołań Socket-ów TCP/IP do postaci protokolarnej charakterystycznej dla jednostek logicznych SNA LU6.2 - w celu realizacji aplikacji zgodnie z modelem klient-serwer.

W przypadku łączenia sieci OSI konieczność użycia bram może być uzasadniona faktem realizacji odmiennych trybów pracy, czyli np. przesyłania datagramów w jednej sieci i zestawiania połączeń wirtualnych w drugiej z sieci OSI.

## 10 Współpraca pakietowych sieci komputerowych z siecią ATM

W chwili obecnej w większości biur, banków, czy instytucji przemysłowych istnieją sprawnie funkcjonujące sieci LAN i MAN. Sieci te działają w oparciu o różne standardy protokolarkie. Do najpopularniejszych z nich należą Ethernet, Token Ring, FDDI. Z kolei wśród protokołów sieciowych opracowanych dla pakietowych sieci komputerowych najpopularniejszym jest protokół IP. Wiele sieci, zarówno rozległych (np. Internet), jak i lokalnych wykorzystuje IP do transferu danych w warstwie sieciowej, mając na uwadze jego niewątpliwe zalety. Coraz mocniej akcentowana jest też potrzeba integracji sieci lokalnych w większe organizmy sieciowe, bądź dołączanie ich do sieci globalnych.

Spełnienie wszystkich postulatów użytkowników, w szczególności zagwarantowanie dużej szybkości transferu danych, wymaga pilnej przebudowy istniejącej infrastruktury komunikacyjnej. Obserwując tendencje rozwojowe w telekomunikacji cyfrowej można przyjąć, że przyszłość w komunikacji sieciowej należeć będzie do szybkiej technologii ATM. Niewątpliwym warunkiem powodzenia ATM będzie jednakże przeźroczystość tej technologii dla protokołów komunikacyjnych sieci lokalnych i rozległych, w tym przede wszystkim protokołów IP i IPX. Nie bez znaczenia dla ewolucyjnych zmian w infrastrukturze podsieci komunikacyjnej jest również zapewnienie możliwości współpracy sieci Frame Relay z ATM.

Z uwagi na powszechność sieci LAN oraz popularność protokołu IP, zarówno ATM Forum, jak i gremia zarządzające Internetem uznały za celowe podjęcie kroków zamierzających do specyfikacji zasad współpracy sieci pakietowych (w tym sieci LAN) z siecią ATM. Prace prowadzone przez ATM Forum oraz IETF zaowocowały opracowaniem dwóch metod, pozwalających na łączenie i współpracę bezpołączeniowych sieci pakietowych LAN, bądź MAN, z połączeniowo zorientowaną siecią ATM. Tym samym sieć ATM może stać się szybką miejską siecią szkieletową dla rozproszonych sieci LAN. Może też być fragmentem sieci Internet.

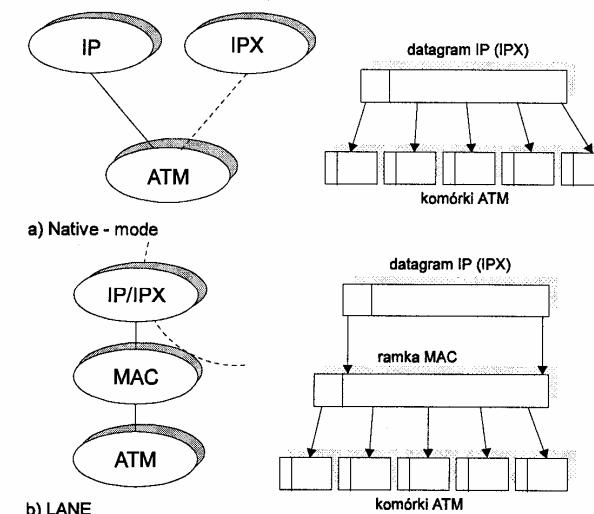
Opracowane metody znane są jako:

- metoda naturalna (ang. *native mode*) współpracy z siecią ATM sieci LAN stosujących te same protokoły sieciowe; w przypadku sieci używających protokołu IP metoda „native mode” określana jest mianem „IP over ATM” (IPoATM): w metodzie „native mode” używane są mechanizmy bezpośredniego odwzorowywania adresów warstwy sieciowej na adresy ATM oraz przekształcania pakietów (datagramów) w komórki ATM; pewnym rozwinięciem metody IPoATM jest koncepcja

współpracy NPOA (ang. *MultiProtocol Over ATM*), dopuszczająca współpracę ATM nie tylko z sieciami TCP/IP ale także z innymi rozwiązaniami firmowymi, w tym np. wykorzystującymi sieciowe systemy operacyjne NetWare z protokołem IPX;

- metoda emulacji sieci LAN na „wierzchołku” architektury ATM, nazywana metodą LAN Emulation (LANE); metoda ta jest bardziej „elastyczna” niż „native mode”, gdyż dopuszcza stosowanie w sieciach LAN wykorzystujących technikę ATM, różnych protokołów sieciowych.

Koncepcje współpracy obu metod (protokołów) z ATM wraz z ilustracją zasad tworzenia komórek prezentuje rysunek 10.1.



Rys. 10.1. Ilustracja metod współpracy sieci LAN/WAN z siecią ATM

Protokół LAN Emulation (LANE) został zaprezentowany przez ATM Forum w styczniu 1995 roku. Funkcjonuje on w podwarstwie MAC i pozwala na łączenie sieci typu Ethernet, czy Token Ring, za pośrednictwem sieci ATM. Szczegółowe implementacyjne LANE są ukryte przed warstwami wyższymi. Dzięki temu nie są wymagane żadne zmiany ani w aplikacjach, ani też w sieciowych systemach operacyjnych (NOS). Zastosowanie protokołu LANE daje użytkownikom sieci LAN możliwość korzystania z dużych przepustowości oferowanych przez ATM. Oprogramowanie LANE zaimplementowane w przełącznikach ATM nie wpływa na ich pracę, gdyż dane protokołu LANE traktowane są jak dane każdego innego połączenia. Z punktu widzenia warstw wyższych stacje sieci Ethernet, Token Ring i ATM komunikują się, jakby były w tej samej sieci LAN. Protokół LANE umożliwia realizację połączeń wirtualnych.

Na rok przed ogłoszeniem propozycji LANE, tj. w styczniu 1994, grupa IETF opublikowała dokument RFC 1577, który zawiera szczegóły specyfikacji nazywanej Classical IP over ATM. Zgodnie z tą specyfikacją możliwa jest integracja sieci ATM z pakietowymi sieciami komputerowymi, stosującymi protokoły TCP(UDP)/IP. Wszystkie aplikacje sieciowe oparte na IP (np. WWW, FTP czy NFS) mogą komunikować się wykorzystując infrastrukturę ATM.

Zarówno LANE jak i IPoATM nie wykorzystują w pełni jednej z najważniejszych cech połączeń ATM, tj. możliwości żądania wymaganej jakości obsługi (ang. QoS - *Quality of Service*). Zastosowanie protokołów LANE lub protokołów typu „native mode” (np. IPoATM) narzuca aplikacjom multimedialnym i innym aplikacjom sieci LAN, uwarunkowanym czasowo, nadzór nad jakością (QoS), realizowanych usług. Oczekuje się, że wprowadzenie IPv6 pozwoli użytkownikom aplikacji Internetu na pełniejsze korzystanie z możliwości ATM. Pomiędzy LANE a IPoATM istnieje dość istotna różnica. LANE z definicji ukrywa własności ATM przed wyższymi warstwami i udaje zwyczajną sieć LAN. Classical IPoATM umożliwia komunikację pomiędzy sieciami LAN przez odwzorowanie adresów warstwy sieciowej na adresy ATM i przenoszenie pakietów warstwy trzeciej w ramkach/komórkach ATM.

## 10.1 Wspieranie protokołu IP przez sieci ATM

W chwili obecnej wiele produktów sieciowych ATM, znajdujących się na rynku, oferuje możliwość instalowania oprogramowania IPoATM. Większość adapterów (kart sieciowych) ATM, routerów ATM i innych urządzeń brzegowych wspomaga specyfikację RFC 1577.

Protokół Classical IPoATM jest prosty koncepcyjnie i łatwy w implementacji. Może on wykorzystywać zarówno połączenia wirtualne stałe (PVC), jak i komutowane (SVC). Zgodnie z ideą protokołu połączenia ATM realizowane są w obrębie tzw. logicznych sieci IP (ang. LIS - *Logical IP Subnetwork*). Zasadnicza część specyfikacji RFC 1577 dotyczy transferu danych w ramach jednej sieci logicznej LIS. Połączenia między różnymi sieciami LIS muszą odbywać się przez routery, nawet jeżeli istnieje fizyczne połączenie ATM między komunikującymi się urządzeniami.

### 10.1.1 Klasyczna wersja protokołu IP over ATM (IPoATM) – RFC 1577

Głównym celem przyświecającym twórcom specyfikacji IPoATM było stworzenie protokołu funkcjonalnie zgodnego ze standardowym IP. Dzięki temu aplikacje już działające mogą korzystać z platformy ATM.

By zapewnić współpracę protokołów warstwy sieciowej typu IP z infrastrukturą ATM, należy rozwiązać dwa zasadnicze problemy: enkapsulacji pakietów oraz odwzorowywania adresów. Istotne znaczenie odgrywają także różnice występujące w połączeniach typu PVC i SVC.

#### 10.1.1.1 Enkapsulacja pakietów (LLC/SNAP)

Celem grupy IETF było zdefiniowanie efektywnej metody przesyłania różnego typu pakietów warstwy sieciowej (i transportowej), przy wykorzystaniu jednego połączenia w sieci ATM, by można było ograniczyć liczbę utrzymywanych połączeń, a ponadto uniknąć opóźnień związanych z każdorazowym nawiązywaniem połączenia. Aby multipleksacja stała się możliwa, stacja docelowa musi rozróżnić typy otrzymywanych pakietów. W związku z tym każdy pakiet poprzedza się identyfikatorem. Ponadto należy określić zasadę enkapsulacji pakietów IP, czyli sposób ich umieszczenia w strukturach danych stosowanych w ATM.

W protokole IPoATM przyjęto enkapsulację typu LLC/SNAP (ang. *Logical Link Control/Subnetwork Access Protocol*). Tym samym multipleksacja pakietów następuje w podwarstwie LLC. Należy więc mówić o enkapsulacji ramek danego standardu sieci LAN (RFC 1577 dopuszcza także inne metody enkapsulacji).

Pakiety IP są dostarczane do warstwy adaptacji ATM - AAL i obsługiwane tam zgodnie z protokołem AAL5, opracowanym z myślą o transferze ruchu, wymagającym obsługi ze zmienną szybkością VBR (głównie ruchu asynchronicznego typu nrt-VBR), względnie ABR. W chwili obecnej, w odniesieniu do ruchu generowanego w większości sieci LAN i MAN, możemy mówić jedynie o świadczeniu usług UBR lub - w ograniczonym zakresie - usług ABR. Jednostki danych tego protokołu (AAL5 PDU) zawierają między innymi nagłówek LLC/SNAP identyfikujący typ pakietu/ramki, pole danych i informacje sterujące AAL5 (długość jednostki PDU i sumę kontrolną CRC).

Dla protokołu IPoATM standardowo przyjęto maksymalną długość pakietów MTU (ang. *Maximal Transmission Unit*) równą 9180 bajtów. Pozwala to na obsługę ramek sieci Ethernet, Token Ring, FDDI, czy SMDS (ang. *Switched Multimegabit Data Service*) bez konieczności ich fragmentacji. Jednocześnie IPoATM dopuszcza, zgodnie ze specyfikacją protokołu AAL5, zwiększenie rozmiaru pakietu do 64 kbajtów. Warto zauważyć, że jest to również maksymalna długość pakietów w sieci Internet. Używanie dłuższych pakietów wpływa na poprawę efektywności transferu. Zwiększenie maksymalnego rozmiaru pakietu wymaga jednakże odpowiedniego skonfigurowania wszystkich stacji sieci LIS.

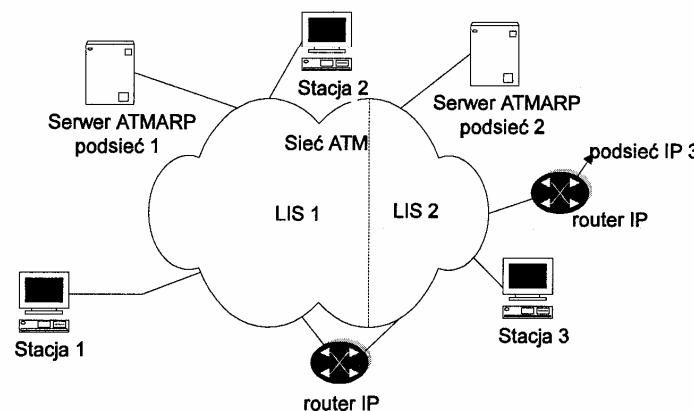
#### 10.1.1.2 Odwzorowanie sieci ATM w logiczną sieć IP – definicja podsieci LIS

W specyfikacji protokołu IPoATM istnieje pojęcie logicznej podsieci IP (ang. LIS - *Logical IP Subnetwork*). Określa ono grupę stacji i routerów dołączonych do jednej sieci ATM i tworzących zamkniętą logiczną podsieć IP.

Podsieć LIS stanowi samodzielnią jednostkę administracyjną sieci ATM. Działa ona i komunikuje się z otoczeniem niezależnie od innych podsieci LIS, zdefiniowanych w tej samej sieci ATM. Urządzenia wewnętrz jednej podsieci LIS komunikują się ze sobą bezpośrednio, przy pomocy połączeń wirtualnych ATM. Stacje

wchodzące w skład LIS nie muszą być umieszczone fizycznie blisko siebie, gdyż na połączenia wirtualne nie są nałożone żadne ograniczenia odległościowe.

Połączenie pomiędzy urządzeniami należącymi do różnych podsieci LIS realizowane jest każdorazowo przez router IP, który należy do jednej lub więcej podsieci LIS i bezpośrednio znajduje się w sieci ATM. To rozwiązanie pozwala na łączenie dużej liczby podsieci LIS w ramach jednej sieci ATM. Podział sieci ATM na dwie podsieci LIS obrazuje rysunek 10.2.



Rys. 10.2. Odwzorowanie sieci ATM w sieć IP

Innym ważnym elementem podsieci LIS jest serwer ATMARP, który prowadzi usługi zamiany adresów IP w ATM. Każda podsieć LIS powinna posiadać jeden serwer ATMARP, dostępny dla wszystkich urządzeń LIS, korzystających z komutowanych połączeń wirtualnych SVC (ang. *Switched Virtual Connection*). Urządzenia te muszą korzystać z tego samego adresu ATM serwera ATMARP. RFC 1577 nie określa w jaki sposób stacje poznają adres swojego serwera. Zazwyczaj konfiguracja wykonywana jest ręcznie, przez operatora sieci.

Urządzenia korzystające z połączeń stałych PVC (ang. *Permanent Virtual Connections*) nie muszą znać adresu serwera ATMARP, gdyż nie stosują usługi zamiany adresu IP w adres ATM.

Dokument RFC 1577 definiuje szereg atrybutów urządzeń należących do jednej podsieci LIS. Są to między innymi:

- taki sam numer podsieci IP oraz maska adresu,
- bezpośrednie połączenie z siecią ATM,
- interfejs odwzorowujący adresy IP w ATM (ATMARP) i odwrotnie - ATM w IP (InATMARP), w przypadku gdy połączenia są typu SVC,
- interfejs odwzorowujący adresy IP w odpowiednie identyfikatory VC, gdy połączenia są typu PVC,

- możliwość komunikowania się z każdą stacją w podsieci LIS poprzez sieć ATM,
- każda stacja IP posiada własny adres ATM oraz dysponuje adresami jednego lub więcej (jeżeli stacja należy do kilku LIS) serwerów ATMARP należących do podsieci LIS.

### 10.1.1.3 Rozwiązywanie problemu adresowania

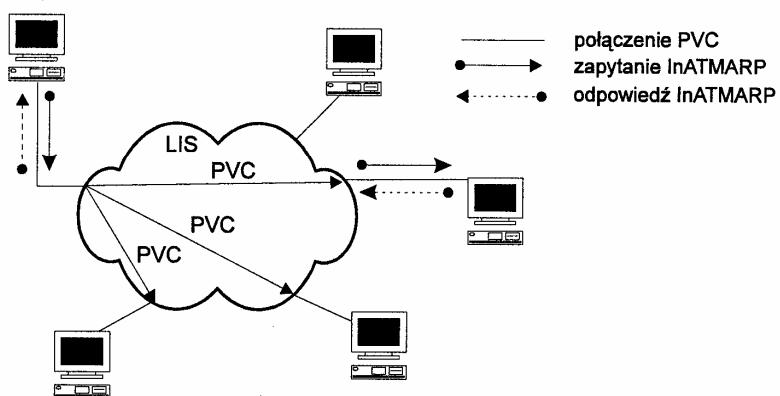
Adresy internetowe urządzeń IP są przydzielane zgodnie z całkowicie odmiennym systemem adresacji od obowiązującego w sieci ATM. Dlatego też w celu zapewnienia prawidłowego operowania protokołu IP na platformie ATM, konieczny jest mechanizm odwzorowywania adresów IP na odpowiadające im adresy ATM (i odwrotnie). Wewnątrz podsieci LIS mechanizm zamiany adresów oparty jest na protokołach:

- ATM Address Resolution Protocol (ATMARP) oraz
- Inverse ATM Address Resolution Protocol (InATMARP).

Oba powyższe protokoły stanowią odpowiedniki internetowych protokołów ARP i InARP. Wszystkie stacje sieci LIS muszą obsługiwać protokoły ATMARP i InATMARP. W tym celu każda stacja posiada własną tablicę adresową, w której przechowuje i jednocześnie uaktualnia najczęściej wykorzystywane adresy ATM. Maksymalny czas przechowywania adresu stacji, od ostatniego uaktualnienia tej informacji, wynosi 15 minut.

W zależności od typu stosowanych połączeń (SVC lub PVC), występują różnice w sposobie odwzorowywania adresów.

#### 10.1.1.3.1 Połączenia PVC



Rys. 10.3a. Przesyłanie zapytania i odpowiedzi InATMARP

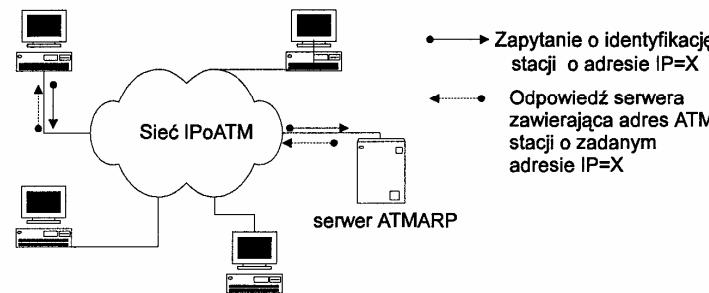
W sieciach ATM ze stałymi połączeniami adresy IP są odwzorowywane w identyfikatory połączeń wirtualnych (ścieżki VPI i kanału VCI). Dla niewielkich podsieci LIS, tablice adresowe stacji można konfigurować ręcznie. Tablica adresowa zawiera pary: adres IP stacji docelowej i identyfikator połączenia wirtualnego. W przypadku większych sieci stacje używają protokołu InATMARP. Każda stacja musi znać połączenia PVC do innych stacji w sieci. W celu ustalenia adresu ATM dla danego połączenia wysyłane jest zapytanie InARP\_REQUEST. Stacja odległa odpowiada pakietem InARP\_REPLY, zawierającym jej adres IP. Sytuacja taka przedstawiona jest na rysunku 10.3a.

#### 10.1.1.3.2 Połączenia SVC – serwery ATMARP

W przypadku realizacji w sieci ATM komutowanych połączeń wirtualnych, odwzorowywanie adresów IP na adresy ATM musi odbywać się automatycznie, tj. na żądanie. Konieczne staje się wówczas korzystanie z serwerów ATMARP. Serwery te utrzymują bazy danych (tablice adresowe) odwzorowujące adresy IP w adresy ATM dla wszystkich stacji w danej podsieci LIS. Fizycznie, serwer ATMARP jest pakietem oprogramowania zainstalowanym na serwerze plików bądź stacji roboczej. Może także rezydować w routerze, względnie przełączniku ATM, w danej podsieci.

Procedura rejestracji nowego urządzenia w podsieci LIS rozpoczyna się od otwarcia połączenia VC typu punkt-punkt do serwera ATMARP. Serwer po wykryciu połączenia od nowego klienta wysyła do niego zapytanie InARP\_REQUEST. Odpowiedź zawiera informacje konieczne do utworzenia nowej pozycji w bazie danych serwera.

W celu utrzymywania aktualnych informacji i minimalizacji rozmiaru tablicy, serwer usuwa pozycje, które nie były używane przez ostatnie 20 minut. Stacje końcowe mogą uniknąć przeterminowania swojego adresu przez utrzymywanie otwartego połączenia do serwera lub okresowe nawiązywanie nowego połączenia (przynajmniej raz na 20 minut).



Rys. 10.3b. Przesyłanie zapytania ATMARP w sieci ATM

Stacja, która chce poznać adres ATM innej stacji wewnętrz podsieci LIS, wysyła zapytanie ARP\_REQUEST, zawierające adres IP, do serwera ATMARP. Sytuacja

taka przedstawiona jest na rysunku 10.3b. Jeżeli serwer znajdzie poszukiwaną pozycję w tablicy adresowej, to odsyła ją w pakiecie ARP\_RESPONSE. W przeciwnym wypadku zwraca ARP\_NAK, aby zasygnalizować brak pozycji dotyczącej zgłoszonego adresu. Zapytania ARP\_REQUEST wykorzystywane są także przez serwer do uaktualnienia zawartości tablicy adresowej.

Warto zauważyć, że w porównaniu z protokołem ARP sieci Internet, nie występuje tu nadmiarowość przesyłanej informacji. W IPoATM zapytanie kierowane jest tylko do jednego serwera, a nie do wszystkich stacji w sieci.

#### 10.1.1.3.3 Format pakietów ATMARP i InATMARP

W pakietach ATMARP i InATMARP zachowano format zbliżony do ich Internetowych pierwowzorów: ARP i InARP. Używane są te same wartości w polach typu adresu, typu protokołu i kodu operacji. Dla zachowania zgodności również położenie wymienionych pól jest takie samo. Pozostała część pakietu zajmuje informacje specyficzne dla sieci ATM. Pakiety ATMARP otrzymały unikatowy typ adresu. Stosowany jest także dodatkowy kod operacji odpowiadający odpowiedzi ARP\_NAK. Format pakietów ATMARP/InATMARP opublikowany w dokumencie RFC 1577, zawarty jest w tabeli 10.1.

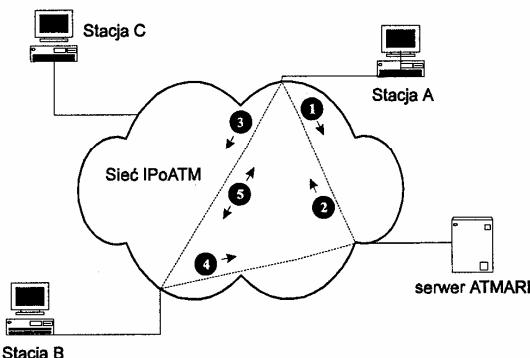
Tabela 10.1. Format pakietów ATMARP/InATMARP wraz z opisem poszczególnych pól

Nazwa pola	długość pola	Opis
ar\$hrd	16 bitów	typ adresu (dla ATM Forum 0x0013)
ar\$pro	16 bitów	typ protokołu (dla IP 0x0800)
ar\$shtl	8 bitów	typ i długość źródłowego numeru ATM (q)
ar\$ssl	8 bitów	typ i długość źródłowego podadresu ATM (r)
ar\$op	16 bitów	kod operacji (ARP_REQUEST, ARP_REPLY, InARP_REQUEST, InARP_REPLY, ARP_NAK)
ar\$spln	8 bitów	długość adresu protokołu źródłowego (s)
ar\$thtl	8 bitów	typ i długość docelowego numeru ATM (x)
ar\$tstl	8 bitów	typ i długość docelowego podadresu ATM (y)
ar\$tpln	8 bitów	długość adresu protokołu docelowego (s)
ar\$sha	q oktetów	źródłowy numer ATM (E.164 lub ATM Forum NSAPA)
ar\$ssa	r oktetów	źródłowy podadres ATM (ATM Forum NSAPA)
ar\$spa	s oktetów	adres protokołu źródłowego
ar\$tha	x oktetów	docelowy numer ATM (E.164 lub ATM Forum NSAPA)
ar\$tsa	y oktetów	docelowy podadres ATM (ATM Forum NSAPA)
ar\$tpa	z oktetów	adres protokołu docelowego

#### 10.1.1.4 Proces nawiązywania połączenia wewnętrz sieci LIS

Rozważmy procesy zachodzące podczas zestawiania połączenia między dwiema stacjami należącymi do tej samej podsieci LIS. Rysunek 10.4 ilustruje sytuację, w której stacje A i B chcą przesyłać sobie nawzajem pakiety.

Kiedy stacja A chce wysłać pierwszy pakiet do stacji B, oprogramowanie ATMARP współpracujące z IP wysyła zapytanie (1) ARP\_REQUEST do serwera ATMARP o adres ATM stacji B. Serwer odszukuje w swojej bazie danych adres ATM odpowiadający adresowi IP zawartemu w zapytaniu i wysyła ten adres w odpowiedzi (2) ARP\_RESPONSE. Stacja A ustanawia bezpośrednie połączenie ATM (typu SVC) ze stacją B (3) i wysyła pakiet danych. Kiedy stacja B chce odpowiedzieć na otrzymany pakiet, także wysyła zapytanie (4) do serwera ATMARP, aby poznać adres ATM nadawcy. Po uzyskaniu tego adresu stacja B zazwyczaj orientuje się, że ma już otwarte połączenie z takim adresem. Wobec tego nie musi ustanawiać nowego połączenia. Od tego momentu możliwa jest dupleksowa, bezpośrednią komunikację między stacjami (5).



Rys. 10.4. Proces łączenia się stacji w ramach podsieci LIS

W obrębie jednej podsieci LIS stacje komunikują się za pośrednictwem wirtualnych połączeń typu punkt-punkt. Pakiety IP są umieszczane w jednostkach PDU protokołu AAL5 w urządzeniach brzegowych sieci ATM. Komórki ATM tworzone z jednostek PDU są następnie przesyłane przez węzły i przełączniki sieci ATM do miejsca ich przeznaczenia lub urządzenia brzegowego sieci ATM. Tam następuje „składanie” komórek w jednostce PDU i odtwarzanie pakietu IP.

Z punktu widzenia warstwy sieciowej (protokołu IP) transmisja przez sieć ATM jest więc jednoetapowa, bez względu na liczbę przełączników uczestniczących w przekazywaniu komórek ATM.

#### 10.1.1.5 Routery w ATM – łączenie stacji należących do różnych LIS

Classical IPoATM nie pociąga za sobą żadnych zmian w konwencjonalnym łączeniu sieci poprzez routery. Pakiety IPoATM przesyłane są na zasadach obo-

wiązujących w Internecie. Ze stacji źródłowej są one przekazywane do routera, a następnie od routera do routera tak długo, aż osiągnięty zostanie adres docelowy. Na całej ścieżce nagłówki IP, jak i nagłówki warstw wyższych, pozostają niezmienione. Zmianie mogą ulec informacje dotyczące zasad enkapsulacji w pod-warstwie MAC.

Rozważmy transmisję danych między dwiema stacjami w dwóch odrębnych podsieciach LIS połączonych routerem. Oprogramowanie IP rozpoznaje sytuację, gdy stacja chce wysłać pakiet pod adres nie należący do danej sieci LIS. W takim przypadku pakiet kierowany jest do routera wyznaczonego dla tej sieci. Wysłanie pakietu poprzedza zazwyczaj zapytanie kierowane do serwera ATMARP o adres ATMowy routera. Stacja nadawcza dokonuje podziału pakietu IP na komórki ATM, a router składa je z powrotem w pakiet IP. Następnie router odczytuje adres IP przeznaczenia pakietu i powtarza cały proces, przesyłając pakiet do stacji docelowej. Wymagane jest więc zestawienie dwóch połączeń wirtualnych oraz segmentacja i scalanie przesyłanego pakietu.

Takie wykorzystanie routerów zapewnia bezpieczeństwo i umożliwia filtrowanie ruchu w sieci. Wpływ ono jednak na obniżenie szybkości transmisji. Dodatkowo routery mogą często pracować w stanie przeciążenia. Można temu zapobiec przez odpowiednie konfigurowanie sieci LIS. Często wykorzystywane, wspólne zasoby sieciowe, takie jak serwery plików, powinny być dołączane do kilku sieci LIS. W rezultacie następuje ograniczenie liczby pakietów przesyłanych przez routery.

#### 10.1.2 Rozszerzenia standardu Classical IP over ATM

Wąskim gardłem klasycznego IPoATM jest brak możliwości bezpośredniej transmisji między różnymi podsieciami LIS. Problem jest poważny, gdyż routery nie są w stanie efektywnie realizować funkcji decydujących o atrakcyjności ATM, tj. zarządzania jakością transmisji (QoS), a także gwarantowania minimalnego opóźnienia i dużej przepustowości.

Aktualnie prowadzone są badania nad bardziej zaawansowanymi implementacjami IPoATM. Grupa Multiprotocol Over ATM, związana z ATM Forum, pracuje nad osadzeniem takich protokołów jak IP, IPX/SPX czy Appletalk w sieci ATM, z pominięciem routerów.

Druga grupa – ROLC (ang. *Routing over Large Clouds*) – wywodząca się z IETF, w kręgu zainteresowania której znajdują się sieci ATM, Frame Relay i SMDS, zajmuje się propozycją protokołu NHRP (ang. *Next Hop Request Protocol*), podobnego do protokołu ATMARP. W przypadku NHRP, odmiennie niż ma to miejsce w protokole ARP, żądanie odwzorowania adresu jest przekazywane z jednego routera ATM do drugiego, aż do osiągnięcia stacji docelowej lub routera brzegowego sieci ATM.

Oddzielnym obszarem prac jest przygotowanie wersji protokołu wykorzystującego mechanizm ogłoszania komunikatów w sieci ATM (ang. *IP multicast over ATM*).

### 10.1.2.1 NHRP – bezpośrednie połączenia między sieciami IP, opartymi na tej samej platformie ATM

W protokole NHRP (ang. *Next Hop Request Protocol*) wprowadza się pojęcie wielodostępnej, nierożgłoszeniowej sieci logicznej – NBMA (ang. *Non Broadcast Multi-Access*). Termin ten obejmuje sieci ATM, Frame Relay i X.25. Wymienione sieci pozwalają na jednoczesne dołączenie wielu urządzeń, nie udostępniając jednak mechanizmów rozgłoszeniowych, jak typowe LANy.

W skład sieci NBMA wchodzą węzły (stacje i urządzenia) należące do tej samej sieci ATM, między którymi możliwe jest zestawienie połączenia wirtualnego ATM, bez żadnych fizycznych lub administracyjnych ograniczeń.

W ramach sieci NBMA możliwe jest wydzielenie wielu regionów samodzielnych administracyjnie – tzw. podsieci logicznych. NHRP pozwala na bezpośrednie połączenia wewnętrz jednej domeny. Natomiast połączenia między różnymi regionami mogą być logicznie blokowane (np. przez implementację oprogramowania typu firewall).

#### 10.1.2.1.1 Serwery NHS

Protokół NHRP zastępuje serwery ATMARP serwerami NHS (ang. *Next Hop Server*). Każda podsieć logiczna posiada własny serwer NHS. Utrzymuje on tablicę adresową odwzorowującą adresy IP w adresy ATM wszystkich stacji należących do danej podsieci. Tablica zawiera także maski adresów sieciowych IP, dostępnych przez routery należące do danej sieci logicznej.

Podobnie jak w przypadku ATMARP, każda nowa stacja musi znać adres serwera NHS danej podsieci IP i wykonać procedurę rejestracji.

Jak do tej pory zadania NHS w niczym nie odbiegają od zadań serwerów ATMARP. Różnica występuje przy próbie zestawienia połączenia między różnymi podsieciemi IP w ramach jednej sieci NBMA. Wówczas serwery NHS zaczynają pracować jak routery.

Grupa ROLC proponuje dwa modele konfiguracji serwerów NHS: statyczny (określany jako *server mode*) i dynamiczny (ang. *fabric mode*).

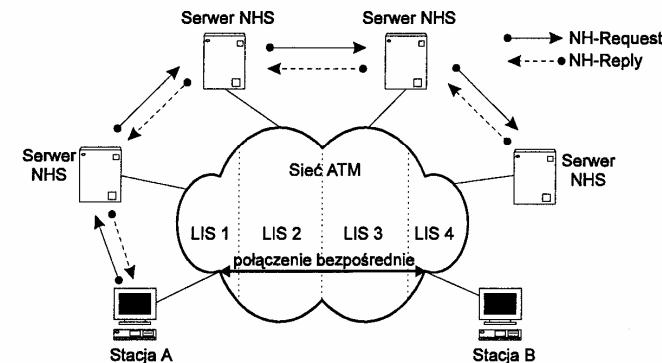
W modelu statycznym każdy NHS jest na stałe wyposażony w tablicę routingu zawierającą maski adresów IP obsługiwanych przez wszystkie inne serwery NHS w sieci NBMA. Takie rozwiązanie jest odpowiednie dla małych sieci – na przykład obsługujących protokół RFC 1577.

Model dynamiczny przewiduje, że serwery NHS będą same budować tablice routingu w oparciu o odpowiednie algorytmy. Zakłada się także, iż na ścieżce wyznaczonej przez algorytm routingu znajdzie się serwer NHS obsługujący daną stację docelową. W praktyce oznacza to, że wszystkie routery wyjściowe sieci NBMA muszą pracować jako serwery NHS dla adresów poza siecią NBMA, osiągalnych z tych routerów. Także routery obsługujące stacje podłączone bezpośrednio do NBMA muszą jednocześnie być ich serwerami NHS.

#### 10.1.2.1.2 Zasada działania protokołu NHRP

Kiedy węzeł w sieci NBMA chce wysyłać pakiet pod adres IP, najpierw kieruje zapytanie (NH-REQUEST) do serwera NHS o adres ATM odbiorcy. Wszystkie komunikaty do i z NHS przesypane są jako pakiety IP.

Jeżeli żądany adres znajduje się w bazie danych serwera, to jest on zwracany w odpowiedzi NH-REPLY. W przypadku braku adresu serwer NHS szuka w tablicy routingu kolejnego serwera NHS na ścieżce wiodącej do stacji docelowej i wysyła tam zapytanie. Proces ten powtarza się, aż do osiągnięcia adresu docelowego, co przedstawia rysunek 10.5. Odpowiedź NH-REPLY wraca zazwyczaj tą samą drogą, którą przesłane było zapytanie. Dzięki temu wszystkie serwery NHS na ścieżce mogą zapamiętać adres stacji docelowej lub (co jest bardziej wartościowe) adres serwera obsługującego podsieć IP o danej masce. Przy kolejnym połączeniu serwer wykorzysta ten adres. Stacja może jednak zażądać wyszukania adresu odbiorcy z pominięciem adresów zapamiętywanych w powyższy sposób (ang. *authoritative mapping*).



Rys. 10.5. Schemat przesyłania zapytań i odpowiedzi między serwerami NHS

Różnego rodzaju mechanizmy mogą być stosowane w celu usuwania nieużywanych adresów i ograniczania w ten sposób liczby przechowywanych pozycji.

Poczas oczekiwania na informację o adresie ATM stacji docelowej pakiety mogą być przesyłane przez routery. Natomiast później zestawia się bezpośrednie połączenie VC między stacjami w ramach sieci ATM. Pojawia się wówczas problem uporządkowania otrzymanych pakietów zgodnie z kolejnością ich nadania. Jednakże większość protokołów warstwy sieciowej z założenia nie gwarantuje tego, pozostawiając kwestie kolejności uporządkowania pakietów warstwom wyższym.

#### 10.1.2.1.3 Bezpieczeństwo i ograniczenia protokołu NHRP

Zasada działania protokołu NHRP pozwala na zestawienie połączenia pomimo zakazów administracyjnych.

W celu rozwiązania problemu bezpieczeństwa i ograniczeń dostępu do zasobów sieci, serwery NHS mogą przesyłać zwrotnie adres odpowiedniego pakietu oprogramowania firewall, zamiast adresu stacji docelowej. Można także zaimplementować filtrację adresów na poziomie sieci ATM, w celu uniemożliwienia zestawienia bezpośredniego połączenia z zewnątrz do danej sieci logicznej.

Niebezpieczeństwem zapamiętywania dróg „na skróty” jest możliwość powstania pętli w systemie routerów. Grupa ROLC zaleca wprowadzenie dodatkowych komunikatów między serwerami NHS, które informowałyby o wykrytych zmianach w topologii routingu. Odpowiedzi NH-Reply zawierają także bit wskazujący, czy dane połączenie będzie stabilne. Jeżeli tak nie jest, to serwery NHS, uczestniczące w wyszukiwaniu adresu ATM, nie powinny zapamiętywać tej trasy.

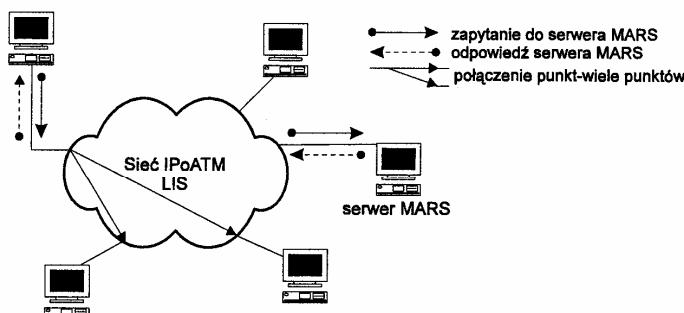
Inną słabością protokołu jest niezdolność do autokonfiguracji, co koliduje z założeniami sieci ATM.

### 10.1.2.2 MARS – multicasting i broadcasting w IPoATM

Standard Classical IPoATM nie umożliwia przesyłania wiadomości do wszystkich użytkowników (typu broadcast) czy grupy użytkowników (typu multicast). Stanowi to główną słabość w porównaniu ze specyfikacją LANE.

Powyższy problem rozwiązyano wprowadzając nowy serwer o nazwie MARS (ang. *Multicast Address Resolution Server*), którego zadaniem jest odwzorowywanie adresów IP typu broadcast i multicast w grupę adresów ATM. Serwer MARS jest ewolucją serwera ATMARP. W bazach danych serwerów MARS realizowane są dwie metody odwzorowywania adresów:

- grupowemu adresowi IP odpowiada lista adresów ATM członków należących do danej grupy (por. rysunek 10.6),

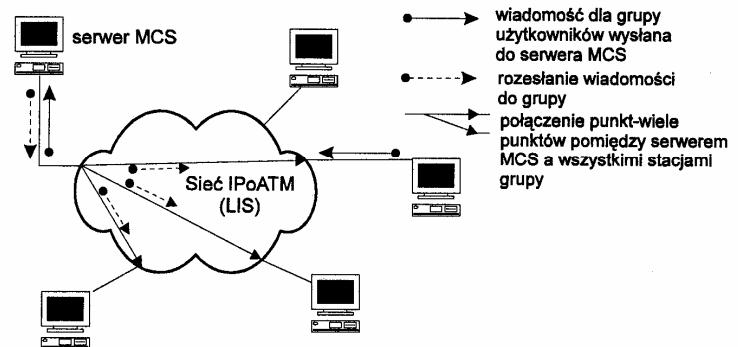


Rys. 10.6. Przesyłanie wiadomości do grupy użytkowników metodą punkt-wiele punktów

- grupowemu adresowi IP odpowiada lista adresów ATM serwerów MCS (ang. *Multicast Server*) obsługujących daną grupę (por. rysunek 10.7).

### 10.1 Wspieranie protokołu IP przez sieci ATM

Stosowanie kilku serwerów MCS dla grupy ma na celu zrównoważenie obciążenia lub/i umyślne wprowadzenie冗undancji. Rozwiązanie to jest nadal przedmiotem badań.



Rys. 10.7. Przesyłanie wiadomości do grupy stacji z wykorzystaniem serwera MCS

W zależności od modelu odwzorowania występują różnice w sposobie rozgłaszenia komunikatów.

#### 10.1.2.2.1 Wysyłanie informacji do grupy użytkowników

Gdy stacja chce rozgłosić wiadomość w grupie, wysyła zapytanie MARS\_REQUEST do serwera MARS, zawierające adres IP tej grupy. Jeżeli MARS nie znajdzie w swojej bazie danych żądanej grupy użytkowników, to wysyła odpowiedź MARS\_NAK. W przeciwnym razie serwer przesyła komunikat MARS\_MULTI. W zależności od metody odwzorowania komunikat zawiera listę adresów ATM stacji należących do grupy lub adres ATM serwera MCS obsługującego grupę.

W pierwszym przypadku stacja, która skierowała zapytanie, zestawia połączenie typu punkt-wiele punktów z otrzymanymi adresami ATM. Staje się wówczas korzeniem tego połączenia i wysyła pakiet. Opisaną sytuację ilustruje 10.6.

W przypadku otrzymania komunikatu zawierającego adres serwera MCS, stacja zestawia z nim połączenie punkt-punkt. Jeżeli stacja chce wysłać wiadomość do grupy, kieruje ją do serwera MCS, który z kolei przesyła ją do wszystkich członków grupy (patrz rysunek 10.7). Jeden serwer MCS może obsługiwać kilka grup, ale musi wtedy umieć rozpoznawać adres grupy według zawartości AAL\_SDU. Taki serwer MCS rejestruje się w serwerze MARS jako serwer MCS dla kilku grup i posiada po jednym połączeniu punkt-wiele punktów dla każdej z grup. Połączenie usuwane jest dopiero w przypadku zakończenia pracy serwera MCS lub, gdy nie ma już żadnych „liści drzewa” (poszczególne stacje po kolejni wyrejestrowały się).

Serwery MARS i MCS mogą dzielić ze sobą fizyczne interfejsy, ale każdy z nich musi mieć własny adres ATM.

Serwer MARS może wysłać wiadomość o zmianie członków grupy. Wśród przesłanych adresów ATM do serwera MCS nowe dodawane są do połączenia jako kolejne liście, a brakujące są usuwane.

Przesyłanie wiadomości do wszystkich użytkowników jest szczególnym przypadkiem przesyłania wiadomości do grupy użytkowników.

Obie opisane wyżej metody posiadają mechanizmy gwarantujące, że cała lista adresowa dotrze do stacji wysyłającej zapytanie MARS\_REQUEST.

#### 10.1.2.2.2 Dłaczanie i usuwanie stacji z grupy

Każda stacja, która chce brać udział w komunikacji typu multicast lub broadcast, musi zarejestrować się w serwerze MARS. W tym celu wysyłany jest komunikat MARS\_JOIN na grupę o adresie IP=0.0.0.0. Serwer MARS dodaje wówczas adres zgłoszającej się stacji do listy stacji obsługiwanych. Lista ta jest używana przy rozmawianiu pakietów w trybie broadcast.

Serwer MARS może obsługiwać więcej niż jedną podsieć LIS. Jednakże w takim przypadku wszystkie rejestrujące się stacje są dopisywane do jednej grupy. Dlatego, aby uniknąć niekorzystnych następstw przy rozmawianiu, rekomendowany jest jeden serwer MARS dla każdej podsieci LIS.

Po rejestracji stacja może dołączyć się do żądanej grupy wysyłając MARS\_JOIN zawierający adres IP tej grupy. Dłaczanie się od grupy następuje po wysłaniu komunikatu MARS\_LEAVE z adresem grupy.

Jeżeli dana grupa nie jest obsługiwana przez serwer MCS, to MARS informuje wszystkich członków grupy o pojawienniu się nowego członka i przesyła jego adres. Każdy z nich dodaje nowy węzeł do swojego połączenia punkt-wiele punktów. Podobnie po odebraniu komunikatu MARS\_LEAVE pozostały członkowie grupy usuwają zbędne połączenie.

Dla grup obsługiwanych przez MCS, MARS przekazuje komunikaty MARS\_JOIN i MARS\_LEAVE do serwera MCS. Serwer ten odpowiednio dodaje lub usuwa jeden węzeł w swoim połączeniu punkt-wiele punktów.

Specjalną grupą stacji stanowią routery multicastowe. Zgodnie z zaleceniem RFC 1112 zobowiązane są one odbierać komunikaty IGMP Report (ang. *Internet Gateway Message Protocol*) z dowolnej grupy. Z tego powodu routery muszą należeć do wszystkich grup i być dołączone do wszystkich serwerów MARS.

Pomimo tego, iż routery muszą należeć do wszystkich grup, tylko do niektórych z nich otwierają połączenia i przesyłają pakiety.

## 10.2 Emulacja sieci LAN w sieciach ATM

Główna funkcją standardu LAN Emulation (LANE) jest, jak sugeruje sama nazwa, emulacja lokalnej sieci komputerowej na wierzchołku struktury ATM. Protokół ten definiuje zasady dopasowania mechanizmów standardów LAN:

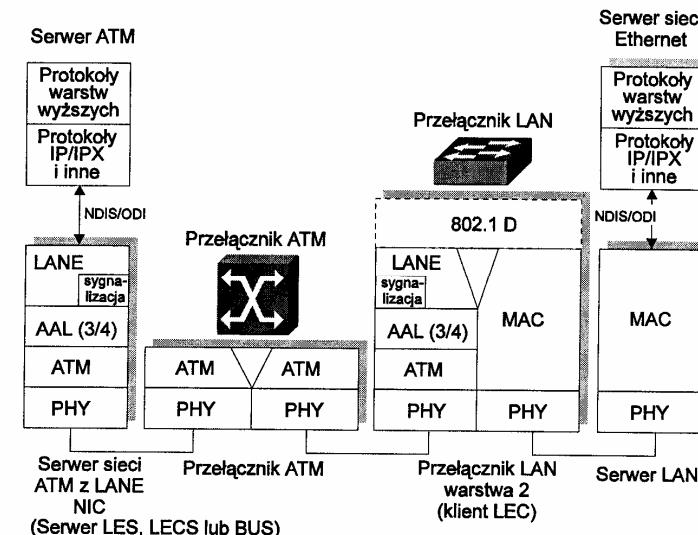
IEEE 802.3/Ethernet i 802.5 Token Ring do wymagań ATM. Nie zostały jednakże sprecyzowane zasady łączenia sieci o różnych standardach w ramach jednej emulowanej sieci LAN. Ich współpraca może być realizowana przy użyciu routera ATM.

Przesłanki, które przemawiają za rozwojem rozwiązań LANE związane są z faktem, że implementacja ATM w formie LAN Emulation nie wymaga żadnej modyfikacji protokołów warstw wyższych. Wynika to między innymi z tego, iż protokoły LANE oferują te same interfejsy użytkowe co protokoły MAC, funkcjonujące w postaci sterowników warstwy sieciowej (NDIS, ODI).

Dane przesyłane przez sieć ATM są umieszczane w komórkach ATM (tj. enkapsulowane do komórek ATM), po uprzednim podziale ramek formatów LAN MAC. Protokoły LANE sprawiają, iż z punktu widzenia użytkownika sieci ELAN sieć ATM zachowuje się tak, jak Ethernet lub Token Ring, chociaż jej funkcjonowanie jest znacznie szybsze.

Protokół LANE umieszczany jest w dwóch typach urządzeń dołączanych do sieci ATM:

- kartach sieciowych sieci ATM (ang. NIC ATM - *Network Interface Card ATM*); jest w nich zaimplementowany protokół LANE oraz interfejs sieciowy ATM,
- urządzeniach do łączenia sieci komputerowych (ang. *Internetworking and LAN Switching Equipment*), czyli routerach (ang. *router*) i przełącznikach (ang. *switch*).

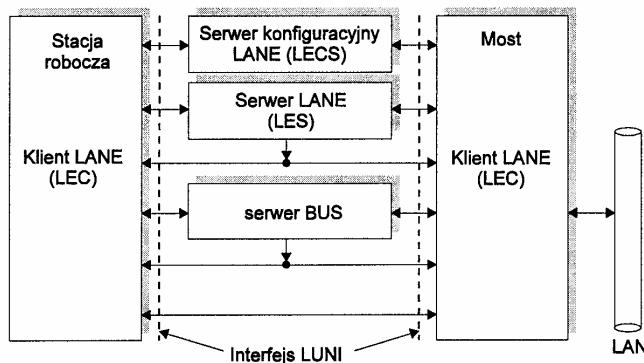


Rys. 10.8. Architektura protokołu LANE

Protokół LANE, jak pokazano na rysunku 10.8, nie wpływa bezpośrednio na funkcjonowanie przełącznika ATM. Działa on niewidocznie przez i nad przełącznikiem, używając tylko standardowych procedur ATM. Podstawową funkcją protokołu LANE jest przeniesienie adresów MAC na adresy ATM.

### 10.2.1 Elementy LANE

Protokół LAN Emulation definiuje operacje na pojedynczych emulowanych sieciach lokalnych, nazywanych tutaj ELAN (ang. *Emulation LAN*, w skrócie - ELAN). Pojedyncza sieć ELAN może być emulowana w standardzie Ethernet lub Token Ring. Oczystym jest fakt możliwości koegzystencji wielu ELAN-ów w jednej sieci ATM. W skład każdej sieci ELAN wchodzą cztery podstawowe elementy (rysunek 10.9), nazywane również obiektami lub komponentami:



Rys. 10.9. Elementy LAN Emulation i ich wzajemne powiązania

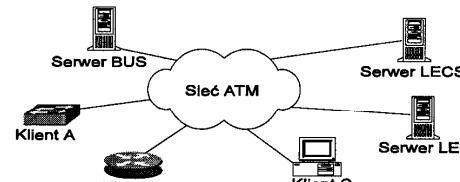
- *LAN Emulation Client (LEC)*: jest to obiekt końcowy systemu ATM. Zakres jego zadań obejmuje między innymi: przesyłanie danych, analizę adresów oraz inne funkcje kontrolne realizowane w ramach pojedynczej sieci ELAN. LEC zapewnia standardowy interfejs użytkownika procesom warstw wyższych. LEC zawiera także interfejs LUNI (ang. *LAN Emulation User Network Interface*) dla komunikacji z innymi elementami LANE. Każdy system końcowy, podłączony do sieci ELAN posiada jeden obiekt LEC na jeden ELAN. Z kolei każdy LEC jest identyfikowany poprzez unikatowy adres ATM i jest związany z jednym lub więcej adresami MAC osiągalnymi poprzez adres ATM. Ta druga sytuacja ma miejsce, gdy klientem LEC staje się most lub przełącznik sieci LAN. Wówczas jeden LEC będzie związany z wszystkimi adresami MAC osiągalnymi poprzez porty tego przełącznika sieci LAN. Należy wziąć pod uwagę i to, że zbiór tych adresów MAC może ulegać dynamicznej zmianie. Obecne specyfikacje LANE definiują dwa

typy sieci ELAN (802.3 i 802.5), nie dopuszczając jednak do bezpośredniego połączenia między klientami LEC, funkcjonującymi w ramach odmiennych standardów LAN, np. LEC z segmentu Ethernet nie może bezpośrednio komunikować się z LEC z Token Ringu. Problem komunikacji pomiędzy tymi dwiema sieciami jest rozwiązywany na poziomie połączeń poprzez router ATM, który funkcjonuje jako klient w każdej z wymienionych sieci ELAN.

- *LAN Emulation Server (LES)*: obiekt implementujący funkcje kontroli w poszczególnych ELANach, posiadający unikatowy adres ATM. Przynależność do danej sieci ELAN oznacza związek z domenowym serwerem LES. LES prowadzi rejestrację adresów stacji sieci ELAN. W tym celu dokonuje analizy i rejestracji adresów MAC stacji a także wyznaczania tych adresów i ich odwzorowywania na adresy ATM (i/lub deskryptory tras do właściwych adresów ATM). W obrębie pojedynczej sieci ELAN może istnieć tylko jeden serwer LES. Górnny limit liczby stacji w sieci ELAN wyznaczany jest poprzez maksymalną liczbę identyfikatorów LEC, które mogą być zarejestrowane w serwerze LES (liczba ta wynosi 65279).
- *Broadcast Unknown Server (BUS)*: wielozadaniowy serwer służący do transmisji pakietów o nieznanym adresie przeznaczenia oraz umożliwiający rozmieszczanie danych, przesyłanie danych do grupy użytkowników jak też obsługę zapytań o nieznane adresy, w ramach jednego ELAN. Każdy klient LEC jest związany z jednym serwerem BUS, ale w ramach jednej ELAN może funkcjonować kilka serwerów typu BUS. Klient LEC rozpoznaje serwer BUS po unikatowym adresie ATM. W serwerze LES wszystkie serwery BUS są związane z jednym adresem MAC.
- *LAN Emulation Configuration Server (LECS)*: serwer prowadzący ewidencję funkcjonujących sieci ELAN wraz z ich podstawowymi parametrami. Każdy obiekt, np. klient LEC, rozpoczętyjący pracę zgodnie z protokołem LANE, musi znać adres serwera LECS. W celu nawiązania połączenia z tym serwerem wysyła on podczas procesu inicjowania połączenia szereg zapytań skierowanych do LECS, chcąc uzyskać informacje między innymi o adresie serwera LES, o wielkości ramki oraz o typie medium. LECS przyporządkowuje klientów LEC do poszczególnych sieci ELAN oraz kieruje ich do odpowiednich serwerów LES. Obecne normy określają istnienie tylko jednego serwera LECS w całej domenie (sieci) ATM, obsługującego wszystkie sieci ELAN. Wersja 2 standardu LANE przewiduje możliwość instalowania kilku serwerów LECS. Informacje przechowywane w serwerze LECS są wprowadzane do niego przez administratora sieci.

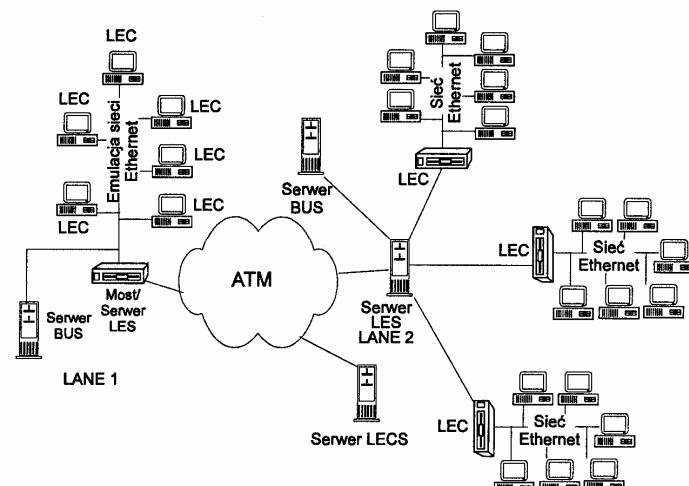
Protokół LANE nie precyzuje, gdzie mają być zlokalizowane wyżej opisane komponenty sieci ELAN. Konieczne jest tylko faktyczne ich dołączenie do sieci ATM (por. rysunek 10.10). Należy się spodziewać, iż wielu producentów zaimple-

mentuje protokół LANE w mostach i przełącznikach sieci LAN. Z kolei serwery ELAN mogą być zaimplementowane w serwerach sieci ATM. Może też zastąpić sytuacja, że wszystkie rodzaje serwerów będą umieszczone w jednym urządzeniu sieciowym, np. routerze. Niezależnie od lokalizacji, każdy z serwerów posiada własny unikatowy adres ATM.



Rys. 10.10. Elementy sieci ELAN

Podana powyżej charakterystyka elementów sieci ELAN jest charakterystyką podstawową. Poszczególne elementy mogą również spełniać dodatkowe funkcje, jak np. inteligentny serwer BUS. Posiada on, podobnie jak serwer LES, tablicę adresów ATM. Dzięki temu wiadomości mogą być przesyłane do konkretnego klienta LEC za pośrednictwem serwera BUS, przez specjalny kanał rozgłoszeniowy, jednakże bez konieczności przesyłania nadmiarowych danych do innych klientów. W tym trybie serwer BUS pracuje jako serwer połączeniowy. Klient może wysyłać wszystkie zapytania do serwera BUS, bez potrzeby podtrzymywania połączeń z innymi elementami sieci ELAN. Serwer BUS może się jednakże wówczas okazać wąskim gardłem systemu.



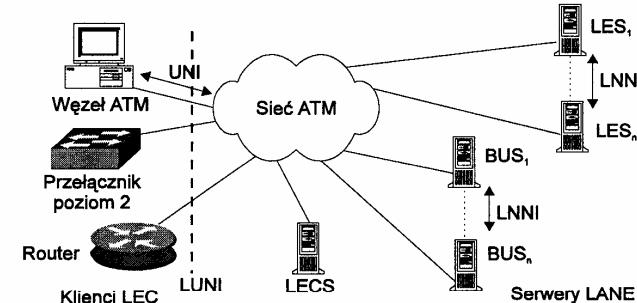
Rys. 10.11. Rodzaje połączeń

Zgodnie z ilustracją zamieszczoną na rysunku 10.11 protokół LANE może obsługiwać jedną sieć LAN (emulacja sieci Ethernet - LANE 1) lub łączyć kilka sieci LAN w jedną sieć wirtualną (LANE 2).

### 10.2.2 Połączenia funkcjonujące w LANE

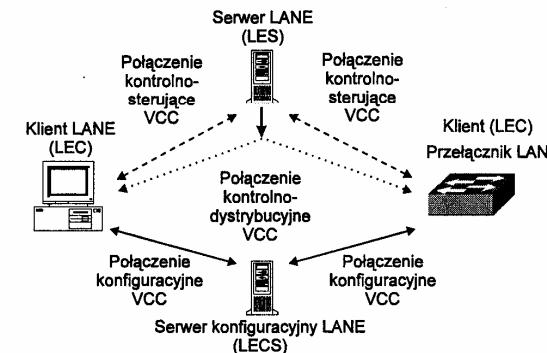
Protokół LANE specyfikuje następujące układy stykowe (rysunek 10.12):

- styk pomiędzy klientem LEC i siecią dostarczającą usługi LANE - LAN Emulation User to Network Interface (LUNI), oraz
- styk pomiędzy serwerami w ramach pojedynczego ELAN - LAN Emulation NNI (LNNI).



Rys. 10.12. Interfejsy protokołu LANE

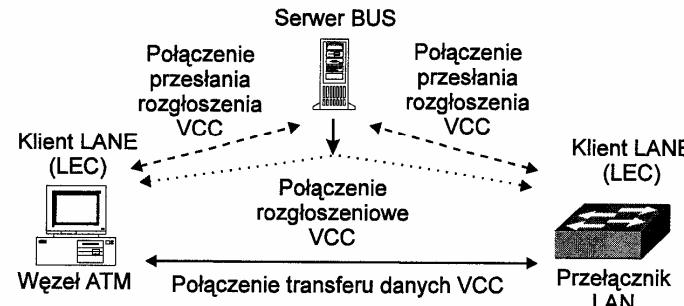
Elementy LANE, których współpraca jest realizowana poprzez LUNI, komunikują się pomiędzy sobą używając adresów ATM. Klient LEC utrzymuje oddzielne połączenia dla transferu danych i kontroli ruchu. Połączenia kontrolno-sterujące nie przenoszą przy tym komórek ATM z ramkami danych i są zestawione w czasie inicjowania pracy klienta LEC w sieci ELAN.



Rys. 10.13. Połączenia kontrolne protokołu LANE

Kontrola ruchu realizowana jest poprzez następujące połączenia (por. rysunek 10.13):

- dwukierunkowe konfiguracyjne połączenie wirtualne (ang. *Configuration Direct VCC*) zestawiane od klienta LEC do serwera konfiguracyjnego LECS; połączenie to może być utrzymywane przez LEC, w czasie jego pracy w sieci ELAN, do przesyłania ewentualnych zapytań do LECS;
- dwukierunkowe połączenie kontrolne (kontrolno-sterujące) (ang. *Control Direct VCC*) ustalane od klienta LEC do serwera LES; połączenie to musi być utrzymywane przez LEC podczas jego pracy w sieci ELAN;
- jednokierunkowe połączenie kontrolno-dystrybucyjne (ang. *Control Distribute VCC*) typu punkt do wielu punktów, od serwera LES do klientów LEC; LES i LEC muszą utrzymywać te połączenia w okresie efektywności klienta LEC.



Rys. 10.14. Połączenia wykorzystywane przy przesyłaniu danych w protokole LANE

Wymiana informacji pomiędzy klientami LEC, bądź między klientem LEC a serwerem BUS, odbywa się za pośrednictwem trzech typów połączeń przesyłania danych (por. rys. 10.14). Są to:

- dwukierunkowe wirtualne połączenie transferu danych VCC (ang. *Date Direct VCC*) zestawiane pomiędzy dwoma klientami LEC, za pośrednictwem którego wymieniane są dane „unicastowe”,
- dwukierunkowe wirtualne połączenie wysyłania rozgłoszenia VCC (ang. *Multicast Send VCC*), realizowane od klienta LEC do serwera BUS,
- jednokierunkowe wirtualne połączenie rozgłoszeniowe (ang. *Multicast Forward VCC*) zestawiane przez serwer BUS do klientów LEC. Jest to typowe połączenie punkt do wielu punktów.

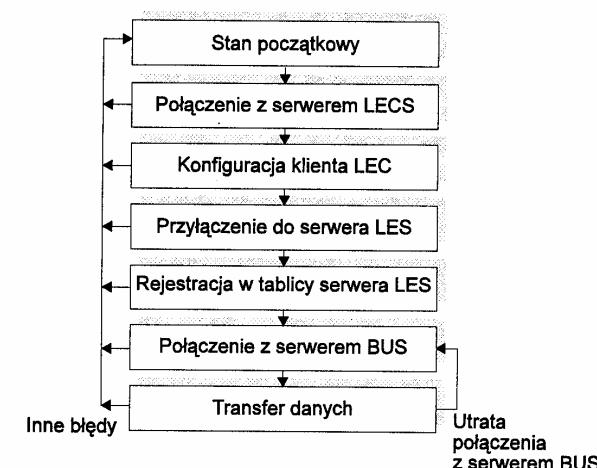
Serwer BUS może przesyłać ramki do klienta LEC bądź przez połączenie MSVCC bądź też MFVCC (jednakże bez dublowania przesyłanych danych).

Należy podkreślić, że połączenia przesyłania danych nie przenoszą informacji sterujących. Wyjątek stanowią jedynie ramki protokołu „flush”.

### 10.2.3 Opis funkcjonowania elementów LANE

Do zestawu czynności (rys. 10.15) wykonywanych przez klienta LEC należą:

- inicjacja pracy,
- konfiguracja klienta,
- połączenie z serwerem LES,
- rejestracja w serwerze LES,
- przesyłanie danych.



Rys. 10.15. Inicjacja, łączenie, rejestracja i przekaz danych w protokole LANE

#### Inicjacja i konfiguracja klienta LEC

Pierwszym krokiem podejmowanym przez klienta LEC w procesie inicjowania jego pracy w danej sieci ELAN jest uzyskanie jego własnego adresu ATM. W tym celu LEC zestawia połączenie konfiguracyjne typu Configuration Direct VCC z serwerem konfiguracyjnym LECS. Aby połączenie to zrealizować, klient LEC musi najpierw określić lokalizację serwera LECS. Czynność tę LEC może wykonać na trzy sposoby:

- poprzez użycie znanego adresu LECS,
- poprzez zestawienie znanego połączenia do LECS (ścieżki i kanału wirtualnego o identyfikatorach VPI=0 i VCI=17),
- poprzez użycie procedury ILMI (ang. *Interim Local Management Interface*), oferującej ograniczony zbiór możliwości protokołu SNMP.

Po zlokalizowaniu serwera konfiguracyjnego LECS, klient LEC ustala połączenie konfiguracyjne. Połączenie to jest następnie używane przez LECS do poinformowania klienta LEC o parametrach obowiązujących w sieci LANE, do której to sieci klient LEC miał być dołączony. Zbiór informacji uzyskiwanych przez klienta LEC składa się między innymi z:

- adresu ATM serwera LES,
- typu emulowanej sieci LAN,
- maksymalnego rozmiaru ramek możliwych do przesyłania w danej sieci ELAN,
- nazwy sieci ELAN.

Ważnym jest fakt, iż według obecnie obowiązujących norm (ang. *LAN Emulation Over ATM Specification - Version 1*), konfigurowanie serwerów LECS jest wykonywane przez administratorów sieci.

#### Działanie i rejestracja klienta LEC

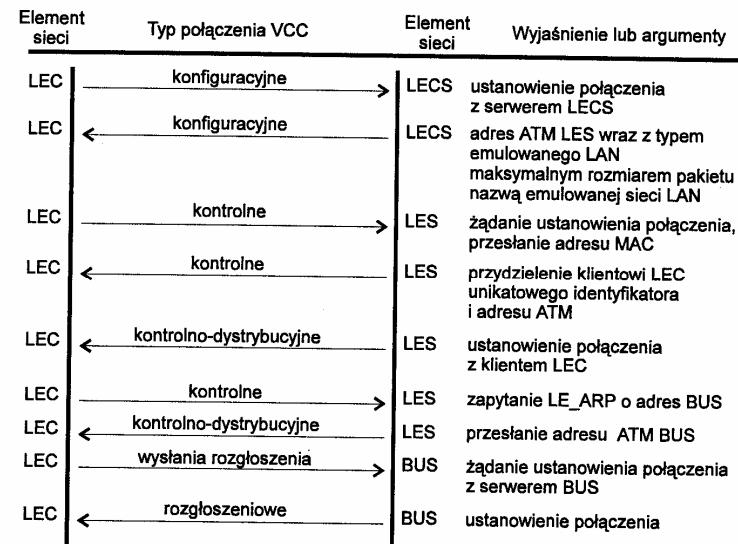
Po uzyskaniu przez klienta LEC adresu serwera LES, klient LEC zwykle zamknie połączenie z serwerem LECS i zestawia wirtualne połączenie kontrolne (kontrolno-sterujące) z serwerem LES i rejestruje w nim własny adres MAC. Korzystając z tego połączenia, serwer LES nadaje klientowi LEC numer identyfikacyjny LECID używany później przy rozgłaszeniu wiadomości oraz przesyła do klienta LEC przypisany mu adres ATM.

W przypadku rejestracji w serwerze LES klienta LEC będącego mostem lub przełącznikiem sieci LAN procedura rejestracji dotyczy zestawu adresów MAC obsługiwanych przez danego klienta.

Równocześnie z rejestracją adresów MAC dokonywana jest przez LEC weryfikacja ich unikalności.

Po rejestracji klienta LEC serwer LES łączy się z klientem połączeniem powrotnym, typu kontrolno-dystrybucyjnego. Tak zestawione połączenia kontrolne i kontrolno-dystrybucyjne są używane przez klienta LEC do uzyskania, za pośrednictwem mechanizmu ARP (tzw. LE\_ARP funkcjonującego w LAN Emulation), adresów ATM odpowiadających poszukiwanym adresom MAC.

Aby zakończyć proces swojej rejestracji, klient LEC używa mechanizmu LE\_ARP do ustalenia adresu ATM serwera BUS. Jest to realizowane przez wysłanie pakietu LE\_ARP, skierowanego do serwera LES na rozgłoszeniowy adres MAC (ang. *broadcast address*) serwera BUS. Serwer LES odpowiada adresem ATM serwera BUS. Po uzyskaniu adresu tego serwera klient LEC inicjuje specjalne połączenie wysłania rozgłoszenia typu multicast send VCC, skierowane do serwera BUS. Serwer BUS odpowiada zestawieniem połączenia rozgłoszeniowego typu multicast forward VCC, skierowanego do klienta LEC. Przykładowy diagram czasowy procesu inicjacji i rejestracji klienta LEC przedstawia rysunek 10.16.

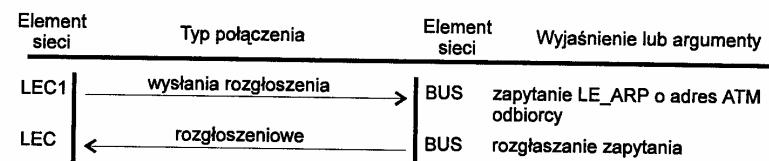


Rys. 10.16. Diagram inicjacji i rejestracji klienta emulacji LANE

Po inicjacji i konfiguracji oraz nawiązaniu stosownych połączeń i rejestracji w serwerze LES, klient LEC jest gotowy do transmisji danych.

#### Transfer danych

W czasie realizacji tej fazy połączenia klient LEC zajmuje się zarówno transportem pakietów do wyższych warstw (poprzez interfejs sieciowy NIC), jak i odbiorem ramek MAC, które mają być przesłane do sieci ELAN. Jeżeli klient LEC, źródłowy, nie zna adresu ATM docelowego klienta LEC, to musi najpierw sformułować i wysłać zapytanie LE\_ARP do serwera LES. Jednocześnie zapytanie LE\_ARP przesyłane jest też do serwera BUS, który rozgłasza je do innych klientów LEC. Ilustruje to rysunek 10.17. Pozwala to na szybsze zlokalizowanie poszukiwanego adresu ATM. Jednocześnie inni klienci mają możliwość „odnotowania” lokalizacji nadawcy.



Rys. 10.17. Ilustracja przesyłania zapytania o adres ATM odbiorcy w przypadku braku odpowiedzi od serwera LES

Podczas oczekiwania na odpowiedź serwera LES, źródłowy klient LEC inicjuje zazwyczaj transfer danych poprzez serwer BUS, używając odpowiednio zdefiniowanej enkapsulacji. Z kolei serwer BUS przesyła odebrane ramki (komórki) danych do klientów LEC. Dublowanie zapytania LE\_ARP (kierowanego do LES i BUS) jest konieczne, ponieważ w sytuacji biernych urządzeń, zlokalizowanych poza przełącznikiem LAN (poza urządzeniem należącym do ELAN), żaden klient LEC nie mógłby wiedzieć, gdzie jest zlokalizowany żądany adres MAC. Wcześniej rozpoczęcie transferu danych za pośrednictwem serwera BUS pozwala ograniczyć, bądź całkowicie wyeliminować:

- straty (gdy warstwy wyższe oprogramowania dokonują odrzucenia pakietu po upływie dopuszczalnego czasu oczekiwania na odpowiedź LE\_ARP), bądź
- opóźnienia (gdy klient LEC dokonuje buforowania pakietu)

w przekazie informacji do adresata.

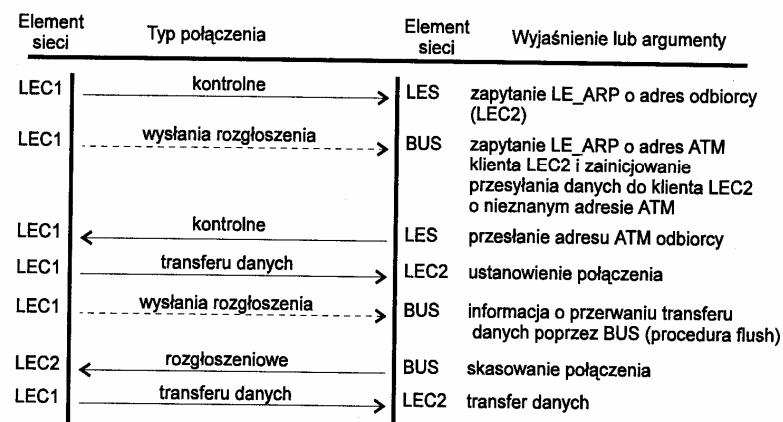
Dla pakietów o nieznanym adresie serwer BUS uaktywnia mechanizm zalewania, używając do tego algorytmu drzewa opinającego (ang. *spanning tree*).

W sytuacji, gdy poprzez realizację mechanizmu LE\_ARP zostanie pozyskany poszukiwany adres, klient LEC zestawia połączenie transferu danych, typu data-direct VCC, z adresem przeznaczenia i wykorzystuje je do przesyłania swoich danych. Zanim jednak to zrobi, LEC może opcjonalnie zrealizować procedurę protokołu LANE o nazwie „flush”, która pozwala upewnić się, iż wszystkie pakiety, które zostały wysłane za pośrednictwem serwera BUS, dotarły do adresata, jeszcze przed inicjacją połączenia transferu danych (ang. *data-direct VCC*). W mechanizmie tym komórka kontrolna jest wysyłana za ostatnim pakietem, pierwszą ścieżką transmisyjną łączącą klienta LEC z serwerem BUS, natomiast drugą ścieżką transmisyjną, łączącą klienta LEC - nadawcę z klientem LEC-odbiorcą, wysyłane są dalsze pakiety danych. Pakiet kontrolny procedury „flush” musi być potwierdzony. Mechanizm ten gwarantuje transmisję, odpowiadającą standardom realizowanym przez mosty LAN, polegającą na zachowaniu kolejności transmitowanych ramek. Przykładową ilustrację wymiany ramek danych pokazuje rysunek 10.18. Klient LEC może również zrezygnować z procedury „flush” uznając, że uporządkowanie ramek w stacji docelowej jest rozwiązaniem korzystniejszym.

Jeżeli wirtualne połączenia transferu danych łączące klienta LEC z poszukiwanymi przez niego adresatami były wcześniej zestawione (i nie zostały usunięte po ostatnich operacjach) i poszczególne adresy MAC są osiągalne, wówczas źródło LEC może opcjonalnie użyć ponownie tych samych połączeń wirtualnych. Pozwoli to na dalsze zachowanie zainicjowanych uprzednio połączeń oraz umożliwi utrzymanie małych opóźnień w transmisji.

W sytuacji, gdy nie ma odpowiedzi na pakiety LE\_ARP, klient LEC będzie kontynuował wysyłanie pakietów danych do serwera BUS, wysyłając też określowo na jego adres zapytania LE\_ARP. Kontynuacja tej czynności trwać będzie

do momentu, aż mechanizm LE\_ARP dostarczy odpowiedzi zawierającej adres ATM odbiorcy. Dzięki tej zwrotnej wiadomości kilku klientów LEC może się „nauczyć” adresu poszukiwanego odbiorcy.



Rys. 10.18. Przesyłanie danych

Każdy klient LEC przechowuje, w postaci tablic, odwzorowania adresów MAC na adresy ATM otrzymane w odpowiedzi na pakiety LE\_ARP. Jeżeli LEC otrzymuje polecenie transmisji innego pakietu, pod ten sam adres MAC, wówczas będzie najpierw poszukiwał adresu ATM w lokalnej tablicy odwzorowań, a następnie, jeżeli nie znajdzie odpowiedniego odwzorowania, użyje mechanizmu LE\_ARP. Zestawy adresów zapamiętanych w tablicach odwzorowań są usuwane po upływie określonego czasu, np. po pięciu minutach. Podobnie, połączenie transferu danych jest anulowane, jeżeli pozostaje nieaktywne przez ustalony opcjonalnie czas, np. przez 20 minut.

Serwer BUS jest również wykorzystywany przez klienta LEC do przesyłania pakietów typu broadcast i multicast. Pakiety te są transmitowane za pośrednictwem serwera BUS do wszystkich (czy też do grupy) klientów LEC. Proces ten jest analogiczny do pokazanego na rysunku 10.17, z tą różnicą, że za pośrednictwem serwera BUS przesyłane są dane, a nie zapytania LE\_ARP. Rozgłoszenie przez serwer BUS danych użytkownika rodzi niebezpieczeństwo otrzymania przez źródłowego klienta LEC kopii wygenerowanych przez niego informacji. Z uwagi na to protokół LANE wymaga, by wszystkie enkapsulowane ramki warstwy MAC były uzupełniane specjalnym prefiksem LECID, nadawanym klientowi LEC podczas jego rejestracji w serwerze LES. Każdy klient LEC dokonuje z kolei filtracji pól adresowych we wszystkich ramkach otrzymywanych z serwera BUS i odrzuca te, których nadawcą jest on sam.

#### 10.2.4 Algorytm drzewa opinającego w protokole LANE

Algorytm drzewa opinającego może być użyty zarówno w ramach pojedynczej sieci ELAN, jak i w każdej konstrukcji sieciowej złożonej z wielu połączonych ze sobą sieci ELAN. Jego funkcjonowanie (analogiczne do realizowanego w połączonych mostami sieciach LAN) rozwiązuje problemy, które mogłyby powstać w przypadku istnienia zapętlonych połączeń, np. wówczas, gdy sieci zewnętrzne w stosunku do LANE są połączone wzajemnie poprzez zewnętrzne mosty. W celu uniknięcia zapętleń poszczególni klienci LEC, w ramach przełączników (bądź mostów) LAN, wymieniają pomiędzy sobą pakiety BPDU.

Jeżeli przełącznik LAN wykryje pętlę, poprzez protokół spanning tree, wówczas w celu jej przerwania wyłącza jeden z zewnętrznych portów lub port ELAN. Protokół drzewa opinającego porównuje koszty poszczególnych połączeń (zwykle proporcjonalne do szybkości transmisji w przyłączonych do nich segmentach), w związku z tym ma tendencję do preferowania portów LANE. Konsekwencją tego jest zamknięcie w pierwszej kolejności portów zewnętrznych. Jednakże, nawet wówczas, gdy port ELAN zostanie zamknięty, możliwe są połączenia poprzez sieci zewnętrzne.

Działanie protokołu spanning tree w obrębie rozbudowanej sieci wielościeżkowej może sprawić, że poszukiwane przez klientów LEC adresy MAC będą dynamicznie zmieniały swoje położenie, a ich osiągalność może okazać się trudna. Dzieje się tak dlatego, gdyż klienci LEC przechowują lokalnie informacje ARP, przez relatywnie długie okresy. Stąd też istnieje niebezpieczeństwo, iż klient LEC może użyć nieaktualnego odwzorowania. Wówczas, wysłane przez niego informacje mogą nie trafić do odbiorcy.

W celu zmniejszenia negatywnych skutków opisanego powyżej problemu, mechanizm LANE został wyposażony w protokół wymiany wiadomości o nazwie LE-Topology-Request. Procedury tego protokołu są generowane przez każdego klienta LEC posiadającego zaimplementowany protokół spanning tree (może to być np. przełącznik ATM). Ich celem jest lokalizacja każdej zmiany zaistniałej w topologii sieci. Klient LEC, który zaobserwował zmianę topologii sieci, wysyła ramkę protokołu LE-Topology-Request do serwera LES, który z kolei rozsyła ją do wszystkich innych klientów LEC. Po otrzymaniu tej informacji, każdy z klientów LEC modyfikuje posiadaną tablicę odwzorowań, jednakże nie przerywa istniejących połączeń transferu danych (ang. *data-direct VCC*). Zmiana w połączeniach następuje dopiero wtedy, gdy mechanizm LE\_ARP nie uaktualni informacji przechowywanych przez klienta LEC. Klient LEC przerywa wówczas połączenie transferu danych.

Protokół LANE pozwala też klientom LEC na generację wiadomości typu LE\_NARP. Są one przesyłane wówczas, gdy klient LEC wykryje nie zarejestrowany, podczas swojego funkcjonowania, adres MAC. Klient LEC wysyła wtedy informację LE\_NARP do wszystkich pozostałych klientów LEC, którzy z kolei wykorzystują tę wiadomość do aktualizacji własnych tablic odwzorowań.

#### 10.2.5 Inteligentny serwer BUS

W standardzie LANE jest wiele problemów „otwartych” na indywidualne rozwiązania producentów. Jednym z nich jest tzw. Inteligentny Broadcast Unknown Server - IB. Inteligentny BUS pozyskuje wiedzę o adresach MAC poprzez dostęp do tablicy adresów w serwerze LES. Dzięki temu IB nie musi zalewać sieci pakietami, których zadaniem jest znalezienie odbiorcy o nieznanym adresie MAC. Może on natomiast przesyłać pakiety do poszukiwanego klienta LEC, wykorzystując tablicę odwzorowania serwera LES, ustalając dwukierunkowe połączenie typu multicast send VCC.

Dzięki możliwości użycia połączenia wysyłania rozgłoszenia, klient LEC przesyła pakiety do serwera BUS, unikając potrzeby wykorzystania innych elementów protokołu LANE. Opcja ta nie jest zalecana przez normy, ponieważ tak pracujący serwer BUS może nie nadążyć z rozsyłaniem otrzymanych informacji.

#### 10.2.6 Łączenie segmentów sieci LAN

Protokół LANE w prawie wszystkich aspektach wydaje się być zwykłym protokołem LAN. Szybkość transmisji w sieci ELAN może być jednakże dużo większa niż w zwykłych sieciach LAN. Dodatkowymi zaletami emulacji jest możliwość tworzenia kilku różnych sieci ELAN w obrębie jednej sieci ATM (domeny). Jeden przełącznik, czy stacja może należeć też do kilku pojedynczych sieci ELAN w obrębie domeny, bez względu na ich fizyczne położenie. Wprowadza się jednakże ograniczenie, polegające na tym, że adapter przełącznika może należeć tylko do jednej sieci. Elementy sieci ELAN nie muszą fizycznie znajdować się w jednym miejscu. Dzięki temu zmiana konfiguracji sieci ELAN nie wymaga fizycznej zmiany lokalizacji poszczególnych elementów.

Kiedy aplikacja stacji końcowej sieci Ethernet lub Token Ring chce wysłać dane do sieci LAN, wysyła ramkę do adaptora sieciowego poprzez standardowy interfejs. Ramka ta zawiera adres MAC odbiorcy, który może być unikatowym adresem stacji końcowej lub adresem rozgłoszeniowym typu broadcast czy multicast. Dalsze czynności obsługi ramki przejmuje adapter z interfejsem emulacji sieci LAN, który:

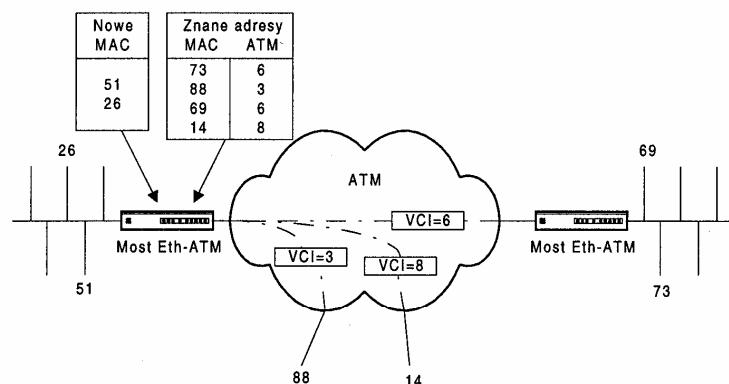
- dla unikatowego adresu MAC sprawdza, czy istnieje już połączenie do odbiorcy. Dane te znajdują się w tablicy adresów MAC;
- jeżeli w tablicy nie ma takiego połączenia, to ustala je zgodnie z procedurami stosowanymi przy transferze danych;
- jeśli połączenie jest ustalone, wówczas adapter do otrzymanej ramki dodaje 2-bajtowy nagłówek emulacji sieci LAN. Tak powstała ramka jest dzielona na segmenty 48-mio bajtowe, do których następnie dołączane są 5-cio bajtowe nagłówki z ustalonymi wartościami VCI/VPI;
- po przesłaniu, komórki są gromadzone i odtwarzane w oryginalne ramki Ethernet/Token Ringu, a następnie przesyłane do aplikacji stacji

końcowej tak, jakby były przesyłane przez sieć lokalną Ethernet czy Token Ring.

LANE może być również użyty do łączenia całych segmentów sieci lokalnych Ethernet lub Token Ring z innymi segmentami, stacjami końcowymi, poprzez sieci ATM. W tym przypadku most lub przełącznik LAN jest widziany przez sieć jako specjalny klient, który reprezentuje wiele różnych adresów MAC. Adresy te są adresami stacji końcowych należących do sieci Ethernet/Token Ring przyłączonych do sieci ELAN.

Wspomniane powyżej mosty i przełączniki LAN muszą posiadać interfejsy emulacji sieci LAN. Po otrzymaniu ramki od stacji końcowej sieci Ethernet lub Token Ring, most (przełącznik LAN) sprawdza, czy ramka ta ma być przesłana na zewnątrz sieci, czy jest przeznaczona dla jednej ze stacji w segmencie lokalnym. Jeśli ramka ma być przesłana dalej, most sprawdza czy dla adresu docelowego MAC istnieje połączenie VC. Od tego momentu proces ustalania połączenia i przesyłania danych jest identyczny jak opisany wcześniej, dla zwykłej stacji końcowej, będącej klientem LANE.

Most, będący specjalnym klientem LEC, rejestrowany jest w tablicach serwera LES jako "pełnomocnik" (ang. proxy). Serwer LES przesyła do niego wszystkie zapytania LE\_ARP. Most musi więc rozpoznawać ramki (komórki) rozgłoszeniowe i rozsyłać je odpowiednio w "swoim" segmencie. Przykład pracy mostu sieci Ethernet w sieci ELAN przedstawiono na rysunku 10.19.



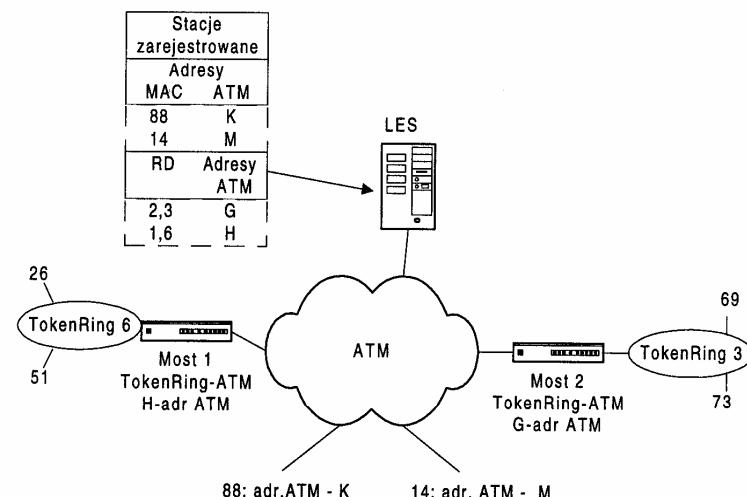
Rys. 10.19. Most sieci Ethernet w sieci ELAN

### 10.2.7 LANE w środowisku sieci Token Ring

W przypadku sieci Token Ring stosowane mogą być dwa rodzaje protokołów transferu ramek: z routingu źródłowym lub bez niego. W przypadku pierwszym,

ramka MAC zawiera pole RI (ang. *Routing Information*), w którym podana jest informacja o poszczególnych sieciach (pierścieniach) i mostach, przez które powinna przejść ramka w drodze od nadawcy do odbiorcy. Klient LEC, przed wysłaniem zapytania LE\_ARP, sprawdza pole RI. Jeśli pole RI nie występuje, lub jest krótsze niż 6 bajtów, lub opis ostatniego pierścienia wskazuje na pierścień klienta LEC, wysyłane jest standardowe zapytanie LE\_ARP z adresem MAC odbiorcy. Kiedy pole RI nie spełnia powyższych warunków, klient LEC przesyła zapytanie LE\_ARP, podając deskryptor routingu RD (ang. *Route Descriptor*), dla następnego kroku, żądanego w polu RI. Działanie to musi być wykonane ze względu na to, że w sieci Token Ring z routingu źródłowym, mosty nie wiedzą nic o adresach MAC urządzeń sąsiednich.

W przypadku rejestracji klienta LEC, będącego mostem sieci Token Ring z routingu źródłowym, serwer LES tworzy dodatkową tablicę deskryptorów RD ze skojarzonymi z nimi adresami ATM. Jeśli serwer LES nie posiada dodatkowej tablicy RD, zapytania LE\_ARP przesyłane są do wszystkich klientów LEC, którzy oznaczeni są jako "pełnomocnicy". Przykładowe tablice adresów MAC, ATM i RD, w środowisku emulacji sieci Token Ring, przedstawione na rysunku 10.20.



Rys. 10.20. Tablice adresów MAC, ATM i RD w środowisku emulowanej sieci Token Ring

### 10.2.8 Uwagi końcowe

Sieci LAN, budowane w oparciu o LANE, dają administratorowi możliwość łatwego i dynamicznego tworzenia sieci wirtualnych oraz śledzenia modyfikacji

zachodzących w grupach roboczych. Innymi słowy - wirtualny LAN pozwala administratorowi adaptować sieć do aktualnych potrzeb organizacyjnych.

Umożliwienie centralnej, logicznej rekonfiguracji elementów systemu, bez konieczności ich fizycznej rekonfiguracji, pozwala na redukcję kosztów związanych z funkcjonowaniem sieci.

Korzyści wynikające z tworzenia wirtualnych sieci LAN z pewnością wpłyną w przyszłości na rozwój standardu LANE. Należy jednak pamiętać, iż rozwiązań to nie eliminuje pewnych wad, które występują w tradycyjnych sieciach LAN. W szczególności, w sieci ELAN może się również pojawić zjawisko zalewania sieci komunikatami, nazywane popularnie sztormami komunikatów (ang. *broadcast storms*) prowadzące w efekcie do wykorzystania standardu ELAN jedynie w małych grupach roboczych. W związku z tym prawdopodobnym wydaje się też, iż firmy posiadające rozbudowane sieci będą zmuszone do tworzenia kilku wirtualnych sieci LAN. Przyjęte w 1995 roku rozwiązanie - LANE wersja 1 - okazuje się pod wieloma względami mało efektywne i nie gwarantujące nawet poziomu usług dostarczanych przez użytkowane dotychczas technologie sieci LAN. W fazie opracowań znajduje się obecnie nowa norma LAN Emulation wersja 2, która definiuje rozproszoną architekturę LAN Emulation, polegającą między innymi na zastosowaniu wielu serwerów konfiguracyjnych. Należy się spodziewać, iż nowelizacja standardu LANE doprowadzi do jego upowszechnienia.

### 10.3 Współpraca sieci Frame Relay i ATM

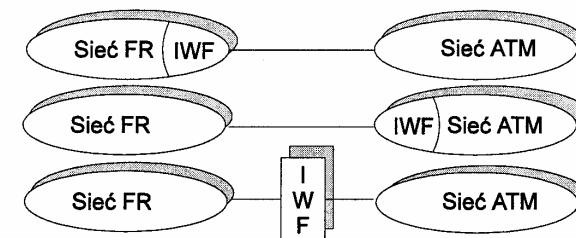
Koncepcja protokołu ATM jest pod wieloma względami podobna do Frame Relay. Oba standardy wykorzystują w pełni wysoką jakość i niezawodność nowoczesnych urządzeń, by zapewnić szybszą komutację pakietów, niż pozwalała na to technologia X.25. Koncepcja kanału wirtualnego w sieci ATM jest też analogiczna do charakterystycznego dla sieci Frame Relay połączenia logicznego. W przypadku obu technologii możliwe jest również multipleksowanie wielu połączeń logicznych w tym samym łączu fizycznym.

#### 10.3.1 Scenariusze współpracy sieci Frame Relay i ATM

Istnieją dwa scenariusze współpracy urządzeń i sieci Frame Relay i ATM:

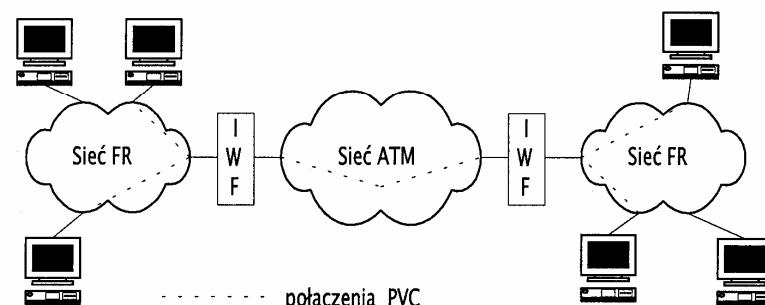
1. łączenie sieci Frame Relay poprzez sieć szkieletową ATM,
2. łączenie użytkowników sieci Frame Relay z użytkownikami sieci ATM, przy założeniu, że żaden z użytkowników nie wie o korzystaniu podczas transmisji z różnych standardów.

Oba rozwiązania są realizowane z wykorzystaniem specjalizowanych układów stykowych definiujących tzw. funkcje współpracy IWF (ang. *Interworking Function*). Możliwa, fizyczna lokalizacja funkcji IWF pokazana jest na rysunku 10.21.



Rys. 10.21. Fizyczne i równoważne lokalizacje styków IWF

W połączeniu dwóch sieci Frame Relay poprzez sieć ATM, wykorzystywana jest enkapsulacja danych. Umożliwia ona „przeźroczystą” transmisję danych użytkowników i sygnalizacji sieci Frame Relay. „Przeźroczystość” oznacza tu, że użytkownicy sieci Frame Relay nie wiedzą, że ich dane przesyłane są poprzez sieć ATM. Rysunek 10.22 przedstawia schematycznie połączenie dwóch sieci Frame Relay poprzez sieć ATM.



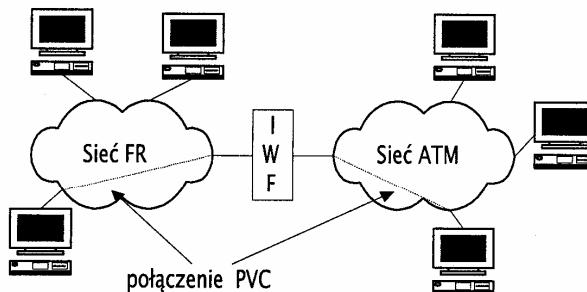
Rys. 10.22. Połączenie sieci Frame Relay poprzez ATM

Układy IWF występują na rysunku 10.22 jako oddzielne jednostki, które mogą być zaimplementowane w przełącznikach sieci ATM lub Frame Relay. Rysunek pokazuje też, że połączenia PVC sieci Frame Relay są odwzorowywane w połączenia PVC sieci ATM. W tym przypadku, wiele połączeń PVC sieci Frame Relay może być multipleksowanych w jednym połączeniu PVC sieci ATM. Istnieje także możliwość odwzorowania każdego połączenia PVC sieci Frame Relay w jedno połączenie PVC sieci ATM.

W drugim scenariuszu współpracy sieci Frame Relay z siecią ATM, styl IWF nie przesyła danych „przeźroczystie”. Funkcje IWF, w tym przypadku, umożliwiają współpracę dwóch różnorodnych standardów.

Jak pokazuje rys. 10.23, połączenie PVC sieci Frame Relay odwzorowywane jest w IWF na połączenie PVC sieci ATM jeden-do-jeden. Nie jest tu możliwa

multipleksacja połączeń PVC. Tak jak w poprzednim przypadku, styk IWF może być zaimplementowany w jednym z przełączników sieci ATM lub Frame Relay.

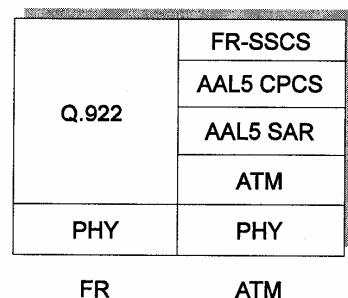


Rys. 10.23. Połączenie sieci Frame Relay z siecią ATM

### 10.3.2 Funkcje IWF

Aby możliwa była współpraca sieci Frame Relay i ATM, styk międzysieciowy IWF musi zapewnić realizację podstawowych funkcji dokonujących enkapsulacji ramki (w przypadku łączenia sieci Frame Relay poprzez ATM) i konwersji nagłówka ramki Frame Relay (gdy transmisja odbywa się pomiędzy użytkownikami sieci Frame Relay i ATM).

Sprzęg IWF implementuje wszystkie funkcje podwarstwy CPCS (ang. *Common Part Convergence Sublayer*) i SAR (ang. *Segmentation and Reassembly Sublayer*) warstwy adaptacji AAL5 ATM. Dodatkowo realizuje funkcje podwarstwy zbieżności dla usług Frame Relay FR-SSCS. Rysunek 10.24 przedstawia umiejscowienie podwarstwy FR-SSCS w warstwowej strukturze styku Frame Relay-ATM.



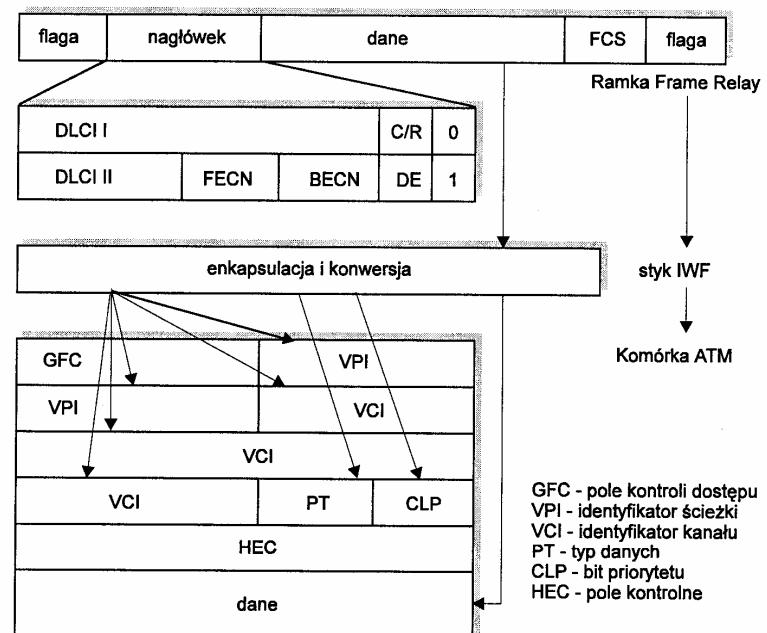
Rys. 10.24. Architektura styku IWF

Zadaniem podwarstwy FR-SSCS jest poprawna interpretacja 2-oktetowego nagłówka ramki Frame Relay (ewentualnie także nagłówków 3 i 4-ro bajtowych)

oraz translacja poszczególnych bitów nagłówka. Jej zadaniem jest również kontrolowanie długości jednostek danych protokołu oraz multipleksacja i demultipleksacja połączeń Frame Relay.

Odwzorowanie nagłówka ramki Frame Relay w nagłówek komórki ATM pokazane jest na rysunku 10.25. W większości przypadków odwzorowanie pól jest obustronne, tzn. jeżeli podczas transmisji z sieci Frame Relay do sieci ATM pole A jest odwzorowywane w pole B, to przy transmisji odwrotnej pole B jest odwzorowywane w pole A. Przykładem odwzorowania obustronnego jest konwersja identyfikatora połączenia logicznego DLCI na identyfikator kanału/ścieżki VCI/VPI, wykorzystywany w komórkach ATM.

W protokole Frame Relay pole DE oznacza bit priorytetu ramki. Spełnia on tę samą rolę co bit CLP w komórce ATM. Odwzorowanie tych pól może być ustalone w dwojakim sposób:



Rys. 10.25. Odwzorowanie nagłówka ramki Frame Relay w nagłówek komórki ATM przez układ IWF

a) przy transmisji z Frame Relay do ATM

- wartość pola DE ramki Frame Relay jest kopipowana do CLP wszystkich komórek ATM, jakie są generowane podczas segmentacji ramki Frame Relay,

- wartość pola DE ramki Frame Relay jest kopiowana do pola DE w nagłówku FR-SSCS PDU, natomiast wartość pola CLP w komórce ATM jest ustalana podczas nawiązywania połączenia i jest stała dla wszystkich komórek tego połączenia,
- b) przy transmisji z ATM do Frame Relay
- jeżeli jedna z komórek „należąca” do ramki Frame Relay (zawierająca część danych ramki Frame Relay) ma bit CLP ustawiony na „1” lub pole DE nagłówka FR-SSCS PDU ma wartość „1”, to pole DE ramki Frame Relay ustawiane jest na „1”,
  - nie istnieją żadne zależności pomiędzy wartościami pola DE ramki Frame Relay, a polem CLP komórki ATM. Pole DE ramki Frame Relay ma wartość pola DE nagłówka FR-SSCS PDU.

Rysunek 10.26 przedstawia zasadę odwzorowywania wartości pola DE ramki Frame Relay w wartość pola CLP komórki ATM i odwrotnie.

a) transmisja z sieci Frame Relay do sieci ATM			b) transmisja z sieci ATM do sieci Frame Relay		
DE FR	DE FR-SSCS	CLP ATM	DE FR	DE FR-SSCS	CLP ATM
0	0	0	0	0	x
1	1	1	1	1	x

Rys. 10.26. Odwzorowanie bitu DE ramki Frame Relay w bit CLP komórki ATM

Odwzorowywanie pól FECN i BECN ramki Frame Relay w pole PT komórki ATM odbywa się następująco:

- a) przy transmisji z Frame Relay do ATM
- wartość pola FECN ramki Frame Relay jest kopiowana do pola FECN nagłówka FR-SSCS PDU. Pole PT komórki ATM nie zostaje ustawione.
- b) przy transmisji z ATM do Frame Relay
- jeżeli pole PT lub pole FECN nagłówka FR-SSCS PDU jest ustawione na „1”, wówczas pole FECN ramki Frame Relay ma wartość „1”.

Schemat odwzorowań pól FECN i PT przedstawiony jest na rysunku 10.27.

Frame Relay do ATM			ATM-do-Frame Relay		
FECN FR	FE-CN FR-SSCS	PT ATM	PT ATM	FE-CN FR-SSCS	FE-CN FR
0	0	0	0	0	0
1	1	0	x	1	1

Rys. 10.27. Schemat odwzorowywania bitu FECN ramki Frame Relay w bit PT komórki ATM i odwrotnie

Bardziej złożone odwzorowanie dotyczy pola BECN ramki Frame Relay. W przypadku transmisji danych z sieci ATM do sieci Frame Relay jest ono ustawiane zgodnie z wartością pola BECN nagłówka FR-SSCS PDU. Natomiast w przypadku transmisji danych z sieci Frame Relay wartość pola BECN nagłówka FR-SSCS PDU ustawiana jest, gdy:

- jest ustawione pole BECN ramki Frame Relay,
- było ustawione pole PT w ostatniej komórce ATM należącej do ramki Frame Relay danego połączenia, przesyłanej w kierunku przeciwnym.

Wymienione odwzorowania oraz konwersja ramek sterowania połączonymi PVC sieci Frame Relay w komórki ATM OAM i odwrotnie umożliwia jednolite zarządzanie połączonymi. W przypadku awarii medium transmisyjnego w jednej sieci, druga sieć jest automatycznie informowana o zdarzeniu.

Również i inne parametry obu sieci wymagają translacji - m.in. informacje sterujące, wynegocjowane parametry ruchu (np. przepływność gwarantowana), itd. Są one ustalane na podstawie algorytmu GCRA (ang. *Generic Cell Rate Algorithm*).

Należy podkreślić, że oba standardy, Frame Relay i ATM, mimo wielu wspólnych cech, wyrosły na różnych fundamentach. Dlatego też połączenie tych standardów i opracowanie zasad ich współpracy rozszerza możliwości dostępu do funkcjonujących w nich aplikacji.

## 11 Uwagi końcowe i wskazówki bibliograficzne

Materiał zaprezentowany w książce obejmuje wybrane problemy pracy sieci komputerowych. Odnoси się on do zasad organizacji i procedur wymiany informacji między obiektami warstwy łączącej danych i warstwy sieciowej w sieciach komputerowych zarówno rozległych jak i lokalnych. Materiał ten podzielić można na pięć zasadniczych części. Część ogólną, obejmującą rozdziały 1 i 2 oraz cztery części szczegółowe.

W rozdziałach 1-2 zaprezentowane zostały podstawowe mechanizmy i procedury związane z funkcjonowaniem sieci komputerowych. Z kolei w rozdziałach 3 - 10 dokonano opisu oraz analizy jakości szerokiego spektrum protokołów komunikacyjnych, mających w przeważającej części znamiona ogólnie akceptowanych standardów.

W rozdziale 3 omówiono przy tym najistotniejsze protokoły warstwy łączącej danych, wykorzystywane w różnorodnych architekturach, opracowanych dla rozległych sieci pakietowych. Z kolei w rozdziałach 4 i 5 zaprezentowano bogatą ofertę standardowych rozwiązań zaprojektowanych dla sieci LAN, zarówno przewodowych (rozdział 4) jak i bezprzewodowych (rozdział 5). Sporo miejsca poświęcono też nowym, wchodzący na rynek rozwiązaniom sieci szybkich, a także rozwiązaniom sieci pozwalającym na świadczenie usług multimedialnych.

Kolejny fragment książki obejmujący rozdziały 6, 7 i 8 zawiera przegląd najważniejszych standardów sieciowych używanych w rozległych sieciach pakietowych.

W rozdziałach 9 i 10 przedstawiono podstawowe zasady i koncepcje łączenia sieci komputerowych, zarówno sprzętowe (rozdział 9) jak i programowe (rozdział 10).

Do książki załączono wykaz używanych w pracy terminów, a także bogatą bibliografię, ilustrującą różnorodne aspekty funkcjonowania sieci komputerowych i systemów rozproszonych. Czytelnika zainteresowanego pogłębieniem wiedzy sieciowej kierujemy też do licznych czasopism fachowych: krajowych i zagranicznych, a także cennych materiałów konferencyjnych, broszur i katalogów firmowych.

Pełne opisy warstwowych architektur logicznych (zaprezentowanych w rozdziale 1 książki) i ich analizy porównawcze znaleźć można między innymi w takich pozycjach jak: A. Tanenbaum [106], [107], D.E. Comer [27], [28], [29], M. Schwartz [94], U. Black [13], F. Hallshal [43], J. Freer [40], a także W. Stallings [102], G. Cole [25] i w wielu innych. Autorzy prac przeglądowych, poświęconych sieciom komputerowym, kładą duży nacisk na wyjaśnienie różnorodnych aspektów funkcjonowania Internetu i zaprezentowanie protokołów tworzących architekturę TCP/IP. Obszerne omówienie tych zagadnień można znaleźć w cy-

towanych powyżej książkach D.E. Comera, A. Tanenbauma (w szczególności w pozycji [107]) oraz licznych materiałach RFC publikowanych przez IETF.

Osoby pragnące zapoznać się z mechanizmami sterowania przepływem danych w sieciach komputerowych, a także podstawowymi protokołami wymiany ramek, stosowanymi w warstwie łączącej danych rozległych sieci pakietowych, kierujemy do publikacji: H. Nusbaumera [79], U. Blacka [13], J.D. Spraginsa (i innych) [100], J. Freera [40], a także M. Schwartza [94], A. Kasprzaka [59] i Z. Papira (i innych) [82].

Szczególnie bogata jest literatura dotycząca zasad funkcjonowania przewodowych sieci LAN i MAN. Różne aspekty pracy tych sieci opisane są w materiałach firmowych i specjalnych wydaniach czasopism fachowych. Godnymi polecenia są też prace: W. Stallingsa [102], [103], [104], A. Tanenbauma [107], a także J. Freera [40], A. Wolisza [112], A.R. Pacha i A. Lasonia [81]. Zainteresowanych tematyką szybkich sieci LAN, w tym sieci gigabitowych odsyłamy do bieżącej literatury fachowej, w tym pozycji [1], [2], [47].

Na rynku wydawniczym brak jest wyczerpujących publikacji poświęconych bezprzewodowym sieciom LAN. Jako referencje dla Czytelnika zainteresowanego tą tematyką polecamy np. pozycje: [42], [48], [51], [86], [87], [113]. Z kolei rozwiązania na temat rozwiązań i możliwości oferowanych przez sieci VSAT znaleźć można w pracach [8], [11], [24], [55], [70] czy też [88].

Rozdziały 6, 7 książki poświęcone zostały opisowi organizacji pracy pakietowych sieci publicznych oraz prezentacji podstawowych technik i standardów komunikacyjnych stosowanych w tych sieciach, a mianowicie: X25, Frame Relay oraz ATM. Problematyka sieci X25 i Frame Relay omawiana jest wyczerpująco np. w pracach: H. Nusbaumera [79], U. Blacka [14], F. Halshalla [43], czy też Z. Papira [82] i A. Kasprzaka [59]. Z kolei opis architektury sieci B-ISDN ATM wraz z przedstawieniem procedur zarządzania i sterowania ruchem w sieciach ATM znaleźć można w książkach: A. Tanenbauma [107], W. Stallingsa [102], a także pracach W. Burakowskiego [20], [21], [22] oraz licznych raportach i opracowaniach np. [9], [10], [90], [91].

Kolejny rozdział książki (rozdział 8) poświęcony został krótkiej prezentacji nowej wersji protokołu IP (IPv6). Czytelnika pragnącego zgłębić tajniki protokołu internetowego IPv6 i nowego schematu adresacji odsyłamy np. do prac D.E. Comera [27], C. Hunta [48], a także np. do pozycji [53] i coraz liczniejszych publikacji w czasopismach.

Znaczny fragment książki poświęcony został zagadnieniom integracji sprzętowej i programowej sieci LAN. Łączenie sieci z wykorzystaniem przełączników, mostów i routerów, omawiane w rozdziale 9, jest zagadnieniem aktualnym, przyciągającym uwagę użytkowników, projektantów i administratorów sieci. Pełniejsze informacje na ten temat można znaleźć w książkach: R. Perlamana [83], A. Tanenbauma [107], J. McConella [66], F. Hallshalla [43] i licznych materiałach

firmowych (np. [3], [4], [5], [6], [18] oraz wielu innych zawartych w bibliografii pozycjach).

Tworzenie wirtualnych sieci LAN, emulacja sieci LAN w sieci ATM, współpraca sieci Frame Relay z siecią ATM, to zagadnienia, którym poświęcony został rozdział 10 książki. Czytelnika zainteresowanego poszerzeniem wiedzy z zakresu tej tematyki kierujemy przede wszystkim do materiałów ATM Forum (np. [108], [109], [110]) oraz stosownych dokumentów RFC i raportów badawczych (np. [60], [61] czy [64]).

Osoby szukające odpowiedzi na podstawowe pytania dotyczące organizacji pracy sieci, w tym sposobów zarządzania i administrowania sieciami komputerowymi, a także typów usług oferowanych przez nowoczesne systemy i sieci teleinformatyczne odsyłamy do pozycji encyklopedycznych, w tym [77] i [98]. Znaleźć tam można zarówno dane techniczne dotyczące nowych generacji systemów i sieci, jak też informacje na temat postępów w standaryzacji sprzętu i oprogramowania sieciowego.

## Bibliografia

1. 100VGAnyLAN/9000. Self-Packed Training Guide. Hewlett Packard, USA, January 1995.
2. 3Com: 100Base-T Fast Ethernet - Strategic Directions. 3Com®, 1995.
3. 3Com: 3Com Technical Papers: Switches and Routers. 3Com®, 1995.
4. 3Com: Boundary Routing and Architecture. 3Com®, 1994.
5. 3Com: Remote Networking., 3Com®, 1994.
6. 3Com: Telenetworking Planning and Implementation Issues. 3Com®, 1994.
7. 3Com: The SuperStack™ System Architecture, 3Com®, 1994.
8. Abramson N.: VSAT Data Networks, Proceedings of IEEE, VOL. 78, NO. 7, July 1990.
9. Alles A.: ATM Internetworking, Cisco System - Engineering InterOp, Las Vegas, 1995.
10. Bąk A.: Reakcyjne metody sterowania ruchem w sieci ATM, rozprawa doktorska, 1997.
11. Bem D.J.: Sieci satelitarne z małymi terminalami, Krajowe Sympozjum Telekomunikacji'93, s. 27-55, Bydgoszcz, 1993.
12. Bertsekas D., Gallager R.: Data Networks, Prentice Hall, 1987.
13. Black U.: Computer Networks, Protocols, Standards and Interfaces, Prentice Hall, Englewood Cliffs, 1993.
14. Black U.: Frame Relay Networks: Specifications and Implementations, 2nd ed., McGraw-Hill Inc., 1995.
15. Black U.: TCP/IP and Related Protocols, McGraw-Hill Inc., 1992.
16. Borman D., Braden R., Jacobsen V.: TCP Extensions for High Performance, RFC-1323, 1992.
17. Boule R., Moy J.: Inside Routers: A Technology Guide for Network Builder in Data Communications, Prentice Hall, 1989.
18. Bradner S.: Testing Network Interconnection Devices, RFC-1242, 1991.
19. Brzeziński K.M.: Sieci lokalne, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 1995.
20. Burakowski W., Bąk A., Kopertowski Z., Kalkowski T.: Szybkie sieci danych, skrypt CITCOM-PW, 1997.
21. Burakowski W.: Inżynieria ruchu w sieciach B-ISDN ATM, Przegląd Telekomunikacyjny nr 7/1993.
22. Burakowski W.: Sieć B-ISDN ATM, Przegląd Telekomunikacyjny nr 5/1993.
23. Callon R.: Use of OSI IS-IS for Routing in TCP/IP and Dual Environments, RFC-1195, 1990.
24. Chakraborty D.: VSAT Communications Networks - An Overview, IEEE Communication Magazine, Vol. 26, No. 5 May 1988.
25. Cole G.: Implementing OSI Networks, J.Wiley, 1991.
26. Coltun R., Fuller V.: The OSPF NSSA Option, RFC-1587, 1994.
27. Comer D. E.: Sieci komputerowe TCP/IP. Zasady, protokoły i architektura, WNT, Warszawa, 1997.

28. Comer D.E., Stevens D.L.: Internetworking with TCP/IP, Vol.I, Prentice Hall, 1991.
29. Comer D.E.: The Internet Book, Englewood Cliffs. Prentice Hall. 1995.
30. Corrigan P., Guy A.: Budowa lokalnych sieci komputerowych Novell NetWare wersje 2.2 i 3.x, Intersoftland, Warszawa 1993.
31. CrossComm: ILANXL Firmware Specification, CrossComm Company, 1994.
32. CrossComm: Router Reference Guide, CrossComm Company, 1995.
33. Distributed Queue Dual Bus (DQDB): Subnetwork of a Metropolitan Area Network. Final Draft DIS, 1990.
34. FDDI - Physical Layer Medium Dependent (PMD) Requirements, 1989.
35. FDDI - Station Management, Draft of International Standard for Information Systems, 1988.
36. FDDI - Token Ring Media Access Control (MAC), Draft of International Standard for Information Systems FDDI, August 1989.
37. FDDI - Token Ring Physical Layer Protocol, Draft of International Standard for Information Systems, 1988.
38. FDDI Hybrid Ring Control (HRC), Draft proposed American National Standard, 1991.
39. Ford L. R., Fulkerson D.R.: Przepływy w sieciach, PWN, Warszawa 1969.
40. Freer J.: Computer Communications and Networks, Pitman 1988.
41. Frish E.: Unix - Administracja systemu, Oficyna Wydawnicza READ ME, Warszawa 1996.
42. Garg V.K., Wilkes J.E.: Wireless and Personal Communications Systems, Prentice Hall, 1996.
43. Hallshal F.: Data Communications, Computer Networks and Open Systems, Addison-Wesley, 1992.
44. Hedrick: Routing Information Protocol, 06/01/1988, RFC 1058.
45. Held G.: Ethernet Networks, J.Wiley, 1994.
46. Held G.: Token-Ring Networks, J. Wiley, 1994.
47. Hewlett Packard: 100VG-AnyLAN, CD-ROM Presentation, HP, 1995.
48. Hołubowicz W., Płociennik P., Różański A.: Systemy łączności bezprzewodowej, Wydawnictwo EFP, Poznań 1996.
49. Huitema C.: Routing in the Internet, Prentice Hall, 1995.
50. Hunt C.: TCP/IP - Network Administration, O'Reilly&Associates, Inc., 1991 (wyd. pol. TCP/IP - Administracja sieci, Oficyna Wydawnicza READ ME, 1996).
51. IEEE 802.11: Wireless Access Method and Physical Specification, DFWMAC: Distributed Foundation Wireless Medium Access Control, IEEE P802.11-93/190. 1993.
52. IEEE 802.3 CSMA/CD Access Method and Physical Layer Specification, IEEE, 1985.
53. IP Version 6 Addressing Architecture, Internet-Draft, 1995.
54. ISO: Basic Reference Model for Open Systems Interconnections, ISO 7498, 1984.
55. ITU (International Telecommunication Union) Handbook on VSAT Systems and Earth Stations, Supplement No. 3 to the ITU Handbook on Satellite Communications; Geneva 1994.
56. Jain R: Performance Analysis of FDDI, Digital Technical Journal vol. 3 No 3 1993.

## Bibliografia

57. Kalkowski T., Bać A., Burakowski W.: Zarządzanie ścieżkami wirtualnymi w sieci B-ISBN ATM, Przegląd Telekomunikacyjny nr 10, 1994.
58. Kalkowski T.: Modelowanie i analiza protokołów warstwy transportowej w sieci ATM, rozprawa doktorska, 1997.
59. Kasprzak A.: Rozległe sieci komputerowe z komutacją pakietów, Wydawnictwo Politechniki Wrocławskiej, Wrocław 1997.
60. Laubach M.: Classical IP and ARP over ATM, RFC 1577, January 1994.
61. Maher M., Mankin A.: ATM Signaling Support for IP over ATM - Uni 4.0 Update, 1996.
62. Malkin G.: RIP Version 2-Carrying Additional Information, RFC-1388, Xylogics, 1993.
63. Mankin A.: The Recomendation for the IP Next Generation Protocol, RFC 1752, Bradner Harvard Univ., 1995.
64. Marshall G.: Classical IP over ATM: A Status Report, Data Commun., December 1995.
65. Martin J., Leben J.: DECnet Phase V. An OSI Implementation, Digital Press, Prentice Hall, 1992.
66. McConnell J.: Internetworking Computer Systems, Prentice Hall, 1988.
67. Metropolitan Area Networks and ATM Technology, International Journal
68. Meyer G.M.: Extensions to RIP to Support Demand Circuits, RFC-1582, 1994.
69. Mills D.: Simple Network Time Protocol (SNTP), RFC-1361, 1992.
70. Minoli D.: Telecommunications Technology Handbook, Artech House, 1991.
71. Moy J.: OSPF Version 2, 03/23/1994, RFC 1583.
72. Moy J.: OSPF Version 2, RFC-1247, 1991.
73. Muller N.J., Davidson R.P.: LANs to WANs. Network Management in the 1990s, Artech House, Boston-London 1990.
74. Muller N.J.: Intelligent Hubs, Artech House, 1993.
75. Naugé M.: Network Protocol Handbook, Prentice Hall, Englewood Cliffs, 1990.
76. NetWorld - roczniki 1995, 1996, 1997.
77. NetWorld - wydanie specjalne: Mała encyklopedia teleinformatyki, 1997.
78. Nunemacher G.: Przewodnik po sieciach lokalnych, ZNI MIKOM, 1996.
79. Nusbaumer H.: Computer Communication Systems, J.Wiley, vol. I; II, 1990.
80. Pach A.R., Lasoń A., Wajda K.: Współpraca sieci ATM z innymi systemami telekomunikacyjnymi, Wyd. Fundacji Postępu Telekomunikacji (WFPT), Kraków 1995.
81. Pach A.R., Lasoń A.: Nowoczesne sieci miejskie, Wyd. Fundacji Postępu Telekomunikacji (WFPT), Kraków 1994.
82. Papir Z. (ed.): Sieci z komutacją pakietów od X.25 do Frame Relay i ATM, Wyd. Fundacji Postępu Telekomunikacji (WFPT), Kraków 1996.
83. Perlman R.: Interconnections - Bridges and Routers, Addison-Wesley, 1992.
84. Popli S.: IsoEthernet - Isochronous Ethernet - The Multimedia LAN for Real Time Desktop Connectivity, National Semiconductor Corporation (www.semiconductors.com)
85. Project 802-Local and Metropolitan Area Networks, Proposed Standard: Distributed Queue Dual Bus (DQDB) Subnetwork over Metropolitan Area Network (MAN), IEEE 802.6, 1990.

86. Radio Equipment and Systems: High Performance Radio Local Area Network (HIPERLAN); ETSI Functional Specification, ver.1.1 RES 10, January 1995.
87. Radio Equipment and Systems: High Performance Radio Local Area Network (HIPERLAN); ETSI Functional Specification, ver.1.1-01 RES 10, March 1996.
88. Rana H., McCoskey J., Check W.: VSAT Technology, Trends and Applications, Proceedings of IEEE, vol. 78, No. 7, July 1990.
89. RFC 1771: A Border Gateway Protocol 4 (BGP-4), 03/21/1995.
90. Roberts J. (ed.): Performance Evaluation and Design of Multiservice Networks, COST 224, October 1991, Directorate General Telecom., Inf. Industries and Innovation 1992.
91. Roberts J., Moccia U., Virtamo J. (eds.): Broadband Network Teletraffic, COST 242, Springer 1996.
92. Sadiku M.N.O.: Metropolitan Area Networks, CRC Press, 1995.
93. Schoffstall M., Fedor M., Davin J., Case J.: A Simple Network Management Protocol (SNMP), RFC-1157, 1990.
94. Schwartz M.: Telecommunication Networks: Protocols, Modelling and Analysis, Addison-Wesley, 1987.
95. Seidler J.: Analiza i synteza sieci łączności dla systemów teleinformatycznych, PWN, 1979.
96. Shah A., Ramakrishnan G.: FDDI: A High Speed Network, Prentice Hall, 1994.
97. Sharma R.: VSAT Network Economics: A Comparative Analysis, IEEE Communications Magazine, February 1989.
98. Sheldon T.: Wielka encyklopedia sieci komputerowych, Wyd. Robomatic, 1995.
99. Sobczak W. (ed.): Problemy Teleinformatyki, WKŁ, Warszawa 1984.
100. Spragins J.D., Hammond J.L., Pawlikowski K.: Telecommunications Protocols and Design, Addison-Wesley, 1991.
101. Stallings W.: Local Area Networks, Macmillan, 3 ed., 1990.
102. Stallings W.: Networking Standards. A Guide to OSI, ISDN, LAN and MAN, 1993.
103. Stallings W.: Data and Computer Communication, Macmillan, 3 ed., 1991.
104. Stallings W.: Local Networks - An Introduction, Macmillan, 1991.
105. Stevens W.R.: Illustrated TCP/IP. Vol.I: Reading, MA: Addison-Wesley, 1994.
106. Tanenbaum A.: Computer Networks, 2 ed., Prentice-Hall. Englewood Cliffs (NJ) 1989.
107. Tanenbaum A.: Computer Networks, 3 ed., Prentice-Hall, 1996.
108. The ATM Forum Technical, Committee LAN Emulation over ATM Version 2 - LNNI, Specification Draft 7, December 1996.
109. The ATM Forum Technical, Interim Local Management Interface (ILMI), Specification Version 4.0, September 1996.
110. The ATM Forum, Committee LAN Emulation over ATM Version 2 - LUNI Specification Draft 4, December 1996.
111. Umar A.: Distributed Computing, A Practical Synthesis, Prentice Hall, 1993.
112. Wolisz A.: Podstawy lokalnych sieci komputerowych, Tom 1,2, WNT, Warszawa 1992.
113. Woźniak J.: Analiza i projektowanie protokołów komunikacyjnych dla radiowych sieci teleinformatycznych, Wyd. Politechniki Gdańskiej, Gdańsk 1991.

## Zestawienie skrótów teleinformatycznych

100Base-T	- 100 Mbps BASEband Twisted pair cable
10Base-2	- 10 Mbps BASEband 2 hundred meter cable
10Base-5	- 10 Mbps BASEband 5 hundred meter cable
10Base-F	- 10 Mbps BASEband Fiber optics cable
10Base-T	- 10 Mbps BASEband Twisted pair cable
10BROAD36	- 10 Mbps BROADband 36 hundred meter
1Base-5	- 1 Mbps BASEband 5 hundred meter cable
AAL	- ATM Adaptation Layer
ABM	- Asynchronous Balanced Mode
ABME	- Extended Asynchronous Balanced Mode
ABR	- Available Bit Rate
ABT	- ATM Block Transfer
ACF	- Access Control Field
Ack	- Acknowledgment
ACK0, ACK1	- positive acknowledgment
ACP	- Advanced Core Protocol
ACR	- Available Cell Rate
ADM	- Asynchronous Disconnected Mode
ADPCM	- Adaptative Differential Pulse Code Modulation
AF	- Arbitrated Functions
AH	- Authentication Header
ANSI	- American National Standards Institute
API	- Application Program Interface
APP C	- Advanced Program to Program Communication
APPN	- Advanced Peer to Peer Networking
ARB	- All-Routes Broadcast
ARCnet	- Attached Resource Computing network
ARM	- Asynchronous Response Mode
ARP	- Address Resolution Protocol
ARPA	- Advanced Research Project Agency
ARPAnet	- Advanced Research Project Agency network
ARQ	- Automatic Repeat reQuest
AS	- Autonomous System
ASCII	- American Standard Code for Information Interchange
ASIC	- Application Specific Integrated Circuit
ASN.1	- Abstract Syntax Notation One

ASP	- Assignment Source Point	CIR	- Cell Injection Ratio
ATM	- Asynchronous Transfer Mode	CLP	- Cell Loss Priority
ATMARP	- ATM Address Resolution Protocol	CLR	- Cell Loss Ratio
AU	- Access Unit	CM	- Connection Management
AUI	- Attachment Unit Interface	CM	- Cycle Master
AUN	- Agent Usługi Nazw	CMC	- Communications Management Configuration
BAA	- Blok Analizy Adresów	CMIP	- Common Management Information Protocol
BCC	- Block Check Character	CMR	- Cell Misinsertion Rate
BCC	- Block Check Code	COCF	- Connection-Oriented Convergence Functions
BCD	- Binary Coded Decimal	ComF	- Common Functions
BECN	- Backward Explicit Congestion Notification	ConF	- Convergence Functions
BER	- Basic Encoding Rules	CP	- Contention Period
BGP	- Border Gateway Protocol	CRC	- Cyclic Redundancy Checking
B-ICI	- Broadband Inter-Carrier Interface	CRM	- Cell Rate Margin
B-ISDN	- Broadband Integrated Services Digital Network	CS	- Configuration Switch
BISYNC	- Binary Synchronous Communications	CS	- Convergence Sublayer
BNP	- Blok Nadzoru nad Połączeniem	CSMA	- Carrier Sense Multiple Access
BPDU	- Bridge Protocol Data Unit	CSMA/CA	- CSMA Collision Avoidance
BRI ISDN	- Basic Rate Interface ISDN	CSMA/CD	- CSMA Collision Detection
BSA	- Basic System Area	C-T	- Cut-Through
BSA	- Blok Selekcji Adresu	CTS	- Clear To Send
BSC	- Binary Synchronous Communication	NCC	- Network Control Center
BSS	- Basic Service Set	DA	- Destination Address
BUS	- Broadcast Unknown Server	DAC	- Dual-Attachment Concentrator
CA	- Channel Allocator	DA-FDMA	- Demand Assignment FDMA
CA	- Collision Avoidance	DAS	- Dual-Attachment Station
CAC	- Connection/Call Acceptance Control	DA-TDMA	- Demand Assignment TDMA
CACS	- Channel Access Control Sublayer	DCE	- Data Circuit - terminating Equipment
CAM	- Continuous - Active Mode	DCE	- Distributed Computer Environment
CBR	- Constant Bit Rate	DCF	- Distributed Coordination Functions
CCIR	- International Consultative Committee on Radio	DDCMP	- Digital Data Communications Message Protocol
CCITT	- Consultative Committee on International Telegraphy and Telephony	DE	- Discard Eligibility
CD	- Collision Detection	DEC	- Digital Equipment Corporation
CDM	- Code Division Multiplexing	DECnet	- Digital Equipment Corporation network
CDMA	- Code Division Multiple Access	DECT	- Digital European Cordless Telecommunications
CDV	- Peak-to-peak Cell Delay Variation	DES	- Data Encryption Standard
CEPT	- The European Conference of Posts and Telecommunications	DFWMAC	- Distributed Foundation Wireless MAC
CER	- Cell Error Ratio	DIFS	- DCF Inter-Frame Space
CFM	- Configuration Management	DLCI	- Data Link Connection Identifier
CFP	- Contention Free Period	DLE	- Data Link Escape
CIDR	- Classless Inter-Domain Routing	DM PDU	- Derived MAC PDU
CIR	- Committed Information Rate	DNA	- Digital Network Architecture

DNIC	- Data Network Identification Code
DNS	- Domain Name System
DPG	- Dedicated Packet Group
DPP	- Demand Priority Protocol
DQDB	- Distributed Queue Dual Bus
DQDB LME	- DQDB Layer Management Protocol
DS SS	- Direct Sequence Spread Spectrum
D-SAP	- Destination SAP
DSL	- Digital Subscriber Line
DTE	- Data Terminal Equipment
DTIM	- Delivery TIM
DTL	- Designated Transit List
EARN	- European Academic and Research Network
EBCDIC	- Extended Binary Coded Decimal Interchange Code
ECM	- Entity Coordination Management
ED	- Ending Delimiter
EFCI	- Explicit Forward Congestion Indicator
EFCN	- Explicit Forward Congestion Notification
EGP	- Exterior Gateway Protocol
EIA	- Electronic Industry Association
EMA	- Enterprise Management Architecture
ENQ	- ENQuiry
EOT	- End Of Transmission
ER	- Explicit Rate
ES	- End Systems
ES	- Express Switching
ESP	- Encapsulated Security Payload
ETB	- End of Transmission Block
ETSI	- European Telecommunications Standards Institute
ETX	- End of Text
FBMT	- Frame Based Management
FC	- Feedback Control
FCS	- Frame Check Sequence
FD	- Frame Discard
FDDI	- Fiber Distributed Data Interface
FDM	- Frequency Division Multiplexing
FDMA	- Frequency Division Multiple Access
FECN	- Forward ECN
FEP	- Front End Processor
F-F	- Fragment-Free
FH SS	- Frequency Hopping Spread Spectrum
FIFO	- First In-First Out

FLP	- Fast Link Pulse
FR	- Frame Relay
FS	- Frame Status
FTP	- File Transfer Protocol
G/I	- Group/Individual
GAN	- Global Area Network
GBN	- Go-Back-N
GCAC	- Generic CAC
GCRA	- Generic Cell Rate Algorithm
GEA	- Gigabit Ethernet Alliance
GFC	- Generic Flow Control
GGP	- Gateway to Gateway Protocol
GMSK	- Gaussian Minimum Shift Keying
Go-Back-N	- GBN
Gopher	- modyfikacja zwrotu Go for it
GOS	- Grade Of Service
HDLC	- High Level Data Link Control
HEC	- Header Error Control
HIPERLAN	- HIgh PErfomance Radio LAN
HMUX	- Hybrid MULTipleXer
HRC	- Hybrid Ring Control
IANA	- Internet Assigned Numbers Authority
ICF	- Isochronous Convergence Functions
ICMP	- Internet Control Management Protocol
IEC	- International Electrotechnical Commission
IEEE	- Institute of Electrical and Electronic Engineers
IETF	- Internet Engineering Task Force
IFS	- Inter-Frame Space
IGP	- Interior Gateway Protocol
ILMI	- Interim Local Management Interface
IM PDU	- Initial MAC PDU
IM	- Initialization Mode
I-MAC	- Isochronous MAC
IMC	- Isochronous Maintenance Channel
IMP	- Interface Message Processors
INC	- INComing
INTERNIC	- INTERnet Network Information Center
IP	- Internet Protocol
I-PNNI	- Integrated Private-Network-to-Network Interface
IPoATM	- IP over ATM
IPX	- Internet Packet Exchange

IPX/SPX	- Internetwork Packet Exchange / Sequenced Packet EXchange
I-S	- Intelligent Switching
IS	- Initialization State
IS	- Intermediate Systems
ISO	- International Standards Organization
ISO-OSI	- ISO Open Systems Interconnection
ITF	- Internet Engineering Task Force
ITS	- Information Transfer State
ITU	- International Telecommunication Union
ITU TSS	- ITU Telecommunication Standardization Sector
ITU-T	- ITU - Telecommunications Sector
LAN	- Local Area Network
LANE	- LAN Emulation
LAP	- Link Access Procedure
LAPB	- Link Access Procedure Balanced
LAPD	- Link Access Protocol on the D-channel
LBR	- Low Bit Rate
LDS	- Logically Disconnected State
LEC	- LAN Emulation Client
LECS	- LAN Emulation Configuration Server
LEM	- Link Error Monitoring
LES	- LAN Emulation Server
LIS	- Logical IP Subnetwork
LLC	- Logical Link Control
LLM	- Link Level Management
LRC	- Longitudinal Redundancy Checking
LU	- Logical Unit
LUNI	- LAN Emulation User Network Interface
MAC	- Medium Access Control
MAN	- Metropolitan Area Network
MAP	- Manufacturing Automation Protocol
MAU	- Medium Attachment Unit
MAU	- Multistation Access Unit
MaxCTD	- Maximum Cell Transfer Delay
MBS	- Maximum Burst Size
MCDV	- Maximum CDV
MCLR	- Maximum CLR
MCR	- Minimum Cell Rate
MCTD	- Maximum CTD
MCU	- Multipoint Control Unit
MD5	- Message Digest 5
MDI	- Media Dependent Interface

MHS	- Message Handling System
MIB	- Management Information Base
MIC	- Medium Interface Connector
MID	- Message Identifier
MII	- Medium Independent Interface
MLP	- Multiple Link Procedure
MMDC	- MultiMedia Desktop Collaboration
MPOA	- Multiprotocol over ATM
MTU	- Maximal Transmission Unit
NAK	- Negative AcKnowledgment
NAV	- Network Allocation
NCP	- Network Control Program
NDIS	- Network Device Interface Specification
NDM	- Normal Disconnected Mode
NetBios	- Network Basic input output system
NFS	- Network File System
NHRP	- Next Hop Request Protocol
NIC	- Network Information Center
NIM	- Network Interface Modul
NJE	- Network Job Entry
NLM	- Network Level Management
NLM	- Node Level Management
NLP	- Normal Link Pulse
NNI	- Network-Network Interface lub Network-Node Interface
NOS	- Network Operating System
NOS	- Network Operating Systems
NP	- Next Page
NPC	- Network Parameter Control
NPDA	- Network Problem Determination Application
NPMA	- Non-preemptive Priority Multiple Access
NPR	- Normal Priority Request
NRM	- Network Resource Management
NRM	- Normal Response Mode
nrt	- non-real-time
nrt-VBR	- non-real-time Variable Bit Rate
NRZ	- Non Return to Zero
NRZI	- Non Return to Zero Inverted
NSP	- Network Services Protocol
OAM	- Operations, Administration and Maintenance
ODI	- Open Data-Link Interface
OSI	- Open Systems Interconnection
OSI RM	- Open Systems Interconnection Reference Model

OSPF	- Open Shortest Path First
P ALOHA	- Pure ALOHA, unslotted ALOHA
PAD	- Packet Assembler-Disassembler
PBX	- Private Branch Exchange
PC	- Personal Computers
PC	- Priority Control
PCF	- Point Coordination Function
PCM	- Physical Connection Management
PCR	- Peak Cell Rate
PCU	- Packet Control Unit
PDH	- Plesiochronous Digital Hierarchy
PDU	- Protocol Data Unit
PHY	- Physical Layer Protocol
PIFS	- PCF Inter-Frame Space
PING	- Packet Internet Grouper
PLP	- Packet Layer Protocol
PLS	- Physical Layer Signalling
PMD	- Physical Medium Dependent
P-NNI	- Private NNI protocol
PPP	- Point to Point Protocol
PS	- Physical Signalling
PSNV	- Power-Save Non-Polling
PSP	- Power-Save-Polling
PSPDN	- Public Switched Packet Data Network
PSTN	- Public Switched Telephone Network
PT	- Payload Type
PT	- Programming Template
PTM	- Packet Transfer Mode
PTPT	- Point to Point Tunneling
PTSE - P-NNI	- Topology State Elements
PTSP - P-NNI	- Topology State Packets
PU	- Physical Unit
PU 2.1	- Physical Unit 2.1
PVC	- Permanent Virtual Circuit
PVC	- Permanent Virtual Connection
QoS	- Quality of Service
RAN	- Random Access with Notification
REJ	- REject
RF	- Remote Fault
RFC	- Request For Comments
RIB	- Routing Information Bit
RIP	- Routing Information Protocol

RM	- Resource Management
RM	- Ring Management
RMON	- Remote MONitoring
RMT	- Ring Management
RNR	- Receive Not Ready
RPC	- Remote Procedure Call
RR	- Receive Ready
RS	- Recommended Standard
RTS	- Request To Send
rt-VBR	- real-time Variable Bit Rate
RVI	- Reverse Interrupt
SA	- Source Address
SAA	- System Application Architecture
SAC	- Single-attachment concentrator
S-ALOHA	- slotted ALOHA
SAPI	- Service Access Point Identifier
SAR	- Segmentation and Reassembly
SAS	- Single-Attachment Station
SAW	- Stop-And-Wait
SCL	- Session Control Layer
SCPC	- Single Channel Per Carrier
SCPC-DAMA	- Single Channel Per Carrier DAMA
SCR	- Sustainable Cell Rate
SD	- Starting Delimiter
SDH	- Synchronous Digital Hierarchy
SDLC	- Synchronous Data Link Protocol
SECBR	- Severely Errored Cell Block Ratio
S-F	- Store-and-Forward
SFD	- Start Frame Delimit
SIFS	- Short Inter-Frame Space
SLIP	- Serial Line Internet Protocol
SLP	- Single Link Procedure
SMDS	- Switched Multimegabit Data Service
SMI	- Structure of Management Information
SMT	- Station Management
SMTP	- Simple Mail Transfer Protocol
SNA	- System Network Architecture
SNA	- System Network Architecture
SNMP	- Simple Network Management Protocol
SOH	- Start Of Header
SONET	- Synchronous Optical Network
SPF	- Shortest Path First

*Zestawienie skrótów teleinformatycznych*

SPX	- Sequenced Packet eXchange	UBR+	- Unspecified Bit Rate+
SRB	- Single-Route Broadcast lub Spanning Tree Explorer	UDP	- User Datagram Protocol
SREJ	- Selective REject	UNI	- User-Network Interface
SRUC	- Split Reservation Upon Collision	UPC	- Usage Parameter Control
S-SAP	- Source SAP	UTP	- Unshielded Twisted Pair
SSCP	- System Service Control Point	VBR	- Variable Bit Rate
STM	- Synchronous Transfer Mode	VC	- Virtual Channel
STP	- Shielded Twisted Pair	VCC	- Virtual Channel Connection
STX	- Start of TeXt	VCI	- Virtual Channel Identifier
SVC	- Switched Virtual Circuit	VCL	- Virtual Channel Link
SVC	- Switched Virtual Connection	VCRP	- Virtual Circuit Routing Protocol
TAM	- Temporary - Active Mode	VF	- Variance Factor
TAPI	- Telephony Application Programmers Interface	VLAN	- Virtual LAN
TAT	- Theoretical Arrival Time	VP	- Virtual Path
TC	- Topology Change	VPC	- Virtual Path Connection
TCA	- Topology Change Acknowledgment	VPI	- Virtual Path Identifier
TCP	- Transmission Control Protocol	VPL	- Virtual Path Link
TCP	- Transmission Control Protocol	VRC	- Vertical Redundancy Checking
TCP/IP	- Transmission Control Protocol/Internet Protocol	VSAT	- Very Small Aperture Terminal
TCU	- Terminal Control Unit	VTAM	- Virtual Telecommunications Access Method
TCU	- Trunk Coupling Unit	WA	- Warstwa Aplikacji
TDD	- Time Division Duplex	WAN	- Wide Area Network
TDM	- Time Division Multiplexing	WBC	- WideBand Channel
TDMA	- Time Division Multiple Access	WLAN	- Wireless LAN
TEI	- Terminal End-point Identifier	WŁD	- Warstwa Łącza Danych
TELNET	- Network Terminal Protocol	WNS	- Warstwa Nadzoru nad Sesją
TFC	- Token Frame Control	WP	- Warstwa Prezentacji
TFTP	- Trivial File Transmission	WPABX	- Wireless PABX
THT	- Token Holding Time	WS	- Warstwa Sesji
TIM	- Traffic Indication Map	WŚ	- Warstwa Sieciowa
TLV	- Type-Length-Value	WT	- Warstwa Transportowa
TOS	- Type Of Service	WWW	- World Wide Web
TP	- Transparent Bridging	XNS	- Xerox Network System
TP-PMD	- Twisted Pair Physical Media Dependent	XTP	- eXpress Transfer Protocol
TR	- Token Ring		
TRT	- Token Rotation Time		
TS	- Traffic Shapping		
TTD	- Temporary Text Delay		
TTL	- Time To Live		
TTRT	- Target Token Rotation Time		
U/L	- Universal/Local		
UBR	- Unspecified Bit Rate		

**100Base-T** (100 Mbps BASEband Twisted pair cable) - standard transmisji i okablowania sieci Ethernet umożliwiające przesyłanie danych z szybkością 100 Mb/s, realizowane za pomocą nieekranowanej skrętki UTP kategorii 3, 4 i 5, ekranowanej skrętki STP lub światłowodów wielomodowych. 100Base-T jest wspierany przez amerykańską organizację producentów produktów sieciowych (*Fast Ethernet Alliance*) z firmami 3Com i Sun Microsystem na czele. Rozwiązywanie to jest technologią zbliżoną do 10Base-T (ten sam format ramki, ta sama metoda dostępu CSMA/CD). Istnieją trzy podstawowe odmiany sieci 100Base-T, każda oparta na innym rodzaju medium transmisyjnego: (1) 100Base-TX stosuje dwie pary skrętek UTP kategorii 5, a maks. długość nie może przekraczać 100 m; (2) 100Base-T4 wykorzystuje cztery pary skrętek kategorii 3, 4 lub 5 przy maks. długości sieci również 100 m.; (3) 100Base-FX oparta na jednym (tryb pół-duplexowy) lub dwóch włóknach (tryb duplexowy) światłowodu wielomodowego. Przyjmuje się, że długość segmentu wynosi typowo 400 m. Możliwe jest też wydłużenie segmentu (odległości między stacją a hubem) do 2 km. Podstawową wadą sieci typu 100Base-T jest ograniczona możliwość ich rozbudowy.

**100VG-AnyLAN** - standard IEEE 802.12 (lansowany głównie przez firmy Hewlett-Packard i IBM) lokalnej sieci komputerowej umożliwiającej przesyłanie danych z szybkością 100 Mb/s. 100VG-AnyLAN pozwala na transmisję ramek Ethernet (IEEE 802.3) lub Token Ring (IEEE 802.5) w istniejącym okablowaniu sieciowym, a więc z użyciem kabli np. UTP kategorii 3 i wyższych. Ponieważ pojedyncza skrętka kategorii 3 nie pozwala na przesyłanie sygnałów z szybkością 100 Mb/s, 100VG-AnyLAN korzysta z czterech par skrętek tego typu. Przez każdą z nich dane są transmitowane z szybkością 25 Mb/s (zastosowanie w sieci kodowania 5B/6B sprawia, że szybkość modulacji w każdej parze wynosi 30 MBodów). Poza kablami UTP, mogą być stosowane kable STP lub światłowody. Topologia sieci jest gwiazdzista lub drzewiasta, z hubem centralnym pierwszego poziomu i maksymalnie dwoma dalszymi poziomami hubów. W sieci zastosowano nową technikę dostępu do medium, tzw. Demand Priority Protocol, wymagającą współpracy stacji z hubami intelligentnymi w podwarstwie MAC. Stacje mogą zgłaszać żądania obsługi o normalnym lub podwyższonym priorytecie. Dostęp do medium uzyskiwany jest przy tym w oparciu o cykliczne przeglądanie interfejsów sieciowych stacji przez hub centralny (przy współpracy z hubami poszczególnych poziomów). Wyklucza to kolizje. Dzięki możliwości nadawania priorytetów przesyłanym danym sieć 100VG-AnyLAN umożliwia (w ograniczonym zakresie) transmisję izochroniczną (dźwięk, wideo). Maksymalny zasięg sieci, uzyskiwany w przypadku użycia światłowodów wielomodowych, wynosi 2000 m.

**10Base-2** (10 Mbps BASEband 2 hundred meter cable) - standard transmisji 10 Mb/s dla sieci Ethernet wykorzystującej cienki kabel koncentryczny; maks. długość pojedynczego segmentu: 185 m przy przepływności 10 Mb/s; maksymalna odległość między dwoma stacjami (z użyciem regeneratorów) wynosi 925 m.

**10Base-5** (10 Mbps BASEband 5 hundred meter cable) - standard transmisji 10 Mb/s dla sieci Ethernet realizowanej za pomocą grubego kabla koncentrycznego („złoty” kon-

centryk); maks. zasięg: 500 m (dla pojedynczego segmentu) przy przepływności 10 Mb/s, z możliwością połączenia do 5-ciu segmentów, o łącznej długości 2,5 km.

**10Base-F** (10 Mbps BASEband Fiber optics cable) - standard transmisji 10 Mb/s dla sieci Ethernet realizowanej za pomocą światłowodów; maks. zasięg: 4600 m przy przepływności 10 Mb/s.

**10Base-T** (10 Mbps BASEband Twisted pair cable) - standard transmisji 10 Mb/s dla sieci Ethernet wykorzystującej pojedynczą parę skręconych przewodów nieekranowych UTP miedzianych; maks. zasięg: 100 m przy przepływności 10 Mb/s.

**10BROAD36** (10 Mbps BROADband 36 hundred meters) - standard transmisji 10 Mb/s dla sieci LAN (Ethernet) wykorzystującej cienki kabel koncentryczny; zapewnia maks. zasięg: 3600 m przy przepływności 10 Mb/s.

**1Base-5** (1 Mbps BASEband 5 hundred meter cable) - standard transmisji 10 Mb/s dla sieci Ethernet realizowanej za pomocą nieekranowanej skrętki symetrycznej UTP lub ekranowanej skrętki symetrycznej STP; maks. zasięg: 500 m przy przepływności 1 Mb/s.

**4B/5B** - kod transmisyjny wykorzystywany w technice światłowodowej, polegający na przyporządkowaniu 4 bitom danych 5-ciu sygnałów elementarnych. Spośród 32 ciągów 5-cio bitowych, możliwych do zapisania w pięciu kolejnych taktach, wykorzystano tylko 25 ciągów kodowych, nie zawierających więcej niż trzy kolejne zera w ciągu; pozostałe ciągi są traktowane jako niedopuszczalne (nielegalne). Kodowanie 4B/5B sprawia, że w dowolnym ciągu przesyłanych bajtów nie ma więcej niż 5 zmian poziomu sygnału do reprezentacji 4 bitów danych. Zapewnia to 80% efektywność kodowania; w porównaniu z kodem transmisyjnym Manchester (o 50% efektywności) kodowanie 4B/5B daje lepsze wykorzystanie dostępnego pasma transmisyjnego i jest stosowane w szybkich sieciach Ethernet i FDDI, umożliwiając uzyskanie użytecznej przepływności 100 Mb/s, przy szybkości modulacji 125 MBodów.

**5B/6B** - metoda kodowania stosowana w technice światłowodowej, a także skrętkowej, polegająca na kodowaniu 5 bitów informacji w 6 taktach zegarowych. Efektywność kodowania - 83%.

**802.X** - grupa standardów IEEE definiująca różne aspekty działania lokalnych sieci komputerowych; standardy z grupy 802.X są akceptowane przez ISO jako standardy serii 8802.x obowiązujące w skali międzynarodowej.

**8B/10B** - metoda kodowania stosowana w technice światłowodowej, polegająca na kodowaniu 8 bitów informacji w 10 taktach zegarowych. Efektywność kodowania: 80%.

**ABR** (*Available Bit Rate*) - usługa o dostępnej szybkości bitowej - przewidziana dla źródeł o niezdefiniowanej szybkości transmisji, umożliwiająca użytkownikowi wykorzystanie, w danym momencie, całej dostępnej przepustowości kanału. ABR zawiera mechanizm kontroli przeciążenia sieci, który zapobiega utracie danych w momentach wzmożonego ruchu. Mechanizm ten po stwierdzeniu, że w sieci jest przeciążenie, zmusza systemy końcowe do zmniejszenia intensywności transmisji lub wręcz wstrzymania przesyłania danych. Tym samym ABR to usługa oferująca zmienne pasmo transmisyjne i nie narzucająca krytycznych wymagań czasowych. Typ ABR usług może być zatem stosowany do obsługi aplikacji nie wymagających gwarantowanego czasu dostarczenia danych do adresata, takich jak np. przekaz plików czy poczta elektroniczna. ABR gwarantuje przy tym (między innymi dzięki zastosowaniu reakcyjnej metody sterowania ruchem) ograniczony poziom strat komórek.

**ABT (ATM Block Transfer)** - usługa blokowego przekazu danych zdefiniowana jedynie przez ITU-T, wykorzystująca ideę dynamicznej rezerwacji pasma przy pomocy komórek zarządzających RM (*Resource Management*). Usługa ta przewidziana jest do obsługi aplikacji generujących dane w postaci bloków o różnych wymaganiach odnośnie pasma. Każda przesyłana porcja danych przedzielana jest komórkami zarządzającymi RM umożliwiającymi wynegocjowanie odpowiedniej szybkości bitowej, do wartości maksymalnej (PCR) szybkości generowania komórek włącznie. Oprócz parametru PCR mogą być również negocjowane parametry dodatkowe jak np. minimalna gwarantowana wartość szybkości.

**adapter liniowy** - urządzenie lub blok komputera, zapewniające współpracę między szyną procesora, a łączem transmisji danych. Adapter przy nadawaniu danych przetwarza dane z postaci równoległej na szeregową, a przy odbiorze odwrotnie. Bierze udział w sterowaniu transmisją i modemem oraz wykonuje część funkcji protokołu liniowego, w tym synchronizację blokową, detekcję błędów transmisyjnych, rozpoznawanie adresów stacji odbiorczej, buforowanie danych itp. Funkcja adaptera liniowego jest implementowana w programowalnych układach dużej skali integracji typu UART (dla - transmisji asynchronicznych) lub USART (dla - transmisji asynchronicznej i synchronicznej). Większość dotychczas stosowanych układów USART (8250,16450) ma maks. szybkość transmisji ograniczoną do 115,2 kb/s; nie wystarcza to szybkim modemom standardu V.34, realizującym kompresję danych.

**adapter sieciowy** - układ instalowany w komputerach PC, „rozszerzający” możliwości podłączenia komputera do sieci lokalnej przez określone medium transmisyjne. Realizuje (najczęściej sprzętowo) funkcje dwóch pierwszych warstw modelu OSI. Każda karta współpracująca ze standardowymi typami sieci lokalnych winna posiadać unikatowy adres MAC, nadawany jej przez producenta (administrowany przez IEEE).

**administrator sieci** - osoba nadzorująca i odpowiadająca za prawidłowe funkcjonowanie sieci. Administrator ma dostęp do wszystkich zasobów sieci oraz uprawnienia umożliwiające kontrolę dostępu i ustalanie uprawnień innych użytkowników sieci do tych zasobów. W pracach związanych z obsługą sieci administrator może wykorzystywać platformy zarządzania sieciami.

**adres** - jeden bądź kilka znaków, jednoznacznie określających i lokalizujących w sieci nadawcę lub odbiorcę przesyłanych danych.

**adresacja sieciowa** - hierarchicznie skonstruowany schemat adresacji gwarantujący dostęp do zasobów sieci poprzez jednoznaczną identyfikację punktów dostępu do usług w warstwie sieciowej modelu ISO-OSI. Użytkownicy otrzymują przy tym niepowtarzalne adresy, zapewniające współpracę sieci prywatnych lub regionalnych za pośrednictwem sieci publicznej, w ramach sieci ogólnosłowiatowej o budowie hierarchicznej. Przy adresowaniu konkretnego punktu na styku DTE/DCE, wg. zalecenia CCITT X.121, ciąg 14-cyfrowy zawiera w sobie numer sieci lub numer międzynarodowy, co umożliwia współpracę przez publiczną sieć telefoniczną, teleksową oraz sieci ISDN. Przyznane przez CCITT kody identyfikacyjne DNIC (*Data Network Identification Code*) dla polskich sieci pakietowych (kod Polski to liczba 260): 2601 Polpak, 2602 Nask, 2603 Telbank, 2607 Cupak, 2604-2606 dla grup sieciowych. Adres sieciowy jest związany z fizyczną strukturą central telefonicznych i przyjmuje alternatywnie jedną z dwóch postaci (np. Polpak): pełną 2601 xxxxxx yyyy lub skróconą 1 xxxxxx yyyy.

**adresacja w sieci Internet** - schemat adresacji gwarantujący jednoznaczne identyfikowanie stacji (komputerów) w sieci Internet poprzez przyporządkowanie każdej stacji

32-bitowego adresu IP składającego się z czterech liczb dziesiętnych oddzielonych kropkami (np. 111.222.133.144). Wartość liczbową każdej z tych czterech części adresu zawiera się w przedziale 0-255. W zależności od potrzeb (liczby podsieci i liczby komputerów) centrum NIC (*Network Information Center*) przydziela klasy A-C narzucające sztywny podział adresu 32-bitowego na część identyfikującą podsieć (*net identifier*) oraz maksymalną liczbę komputerów (host identifier) w podsieci. Dowolną stację w sieci Internet można adresować zarówno przez numer adresowy jak też nazwę, korzystając z konwersji dokonywanej przez serwer adresowy DNS. Nazwę komputera i sieci ustala sam użytkownik w porozumieniu z lokalnym administratorem. Serwery adresowe DNS, zarządzające systemem nazw, dokonują automatycznie konwersji nazwy symbolicznej na numer adresowy, zgodny z protokołem IP (*Internet Protocol*). W przypadku adresów symbolicznych niektóre części adresu mają już określoną przynależność organizacyjną, niezależnie od ich położenia geograficznego. Oprócz domen instytucjonalnych (edu - domena edukacyjna, com - domena komercyjna, mil - domena wojskowa, gov - domena rządowa, org - domena organizacyjna), funkcjonują domeny kraju, miasta, firmy a nawet komputera. Adresy w Internecie dzielone są na klasy A, B, C. Polsce przydzielano dotychczas klasy C (do 254 stacji w sieci) i klasę B (ponad 65 tys. stacji). Najnowsza generacja protokołu Internetu IPv6 wprowadza szereg zmian m.in. zwiększa przestrzeń adresową przeznaczoną do identyfikacji przyłączonych komputerów poprzez użycie adresacji 128-bitowej. Teoretycznie daje to możliwość przydzielenia średnio 1500 adresów na jeden metr kwadratowy Ziemi. Ocenia się, że przejście na nową, rozszerzoną adresację w sieci Internet zajmie najbliższe dwa lata.

**agent** - proces (wykonywany program) działający w węźle sieciowym (stacja robocza, serwer, zasilacz UPS, modem, hub, most, przełącznik, router), który umożliwia monitorowanie oraz zarządzanie pracą tego węzła. Przykładowo agent SNMP w routerze umożliwia wymianę informacji (np. o wielkości ruchu) i zdalne sterowanie pracą routera za pomocą aplikacji zarządzającej opartej na SNMP.

**agent zastępczy (proxy agent)** - procedura konwersji standardowego protokołu SNMP na postać niestandardową, zrozumiałą dla węzła sieci LAN. Umożliwia monitorowanie i kontrolę elementów sieci nie posiadających trybu pracy SNMP. Agent zastępczy jest lokalizowany w dowolnym węźle sieci lub bezpośrednio w stacji zarządzającej siecią.

**agregowane pasmo** - całkowite pasmo kanału służące do transmisji multipleksowanego strumienia danych.

**algorithm spanning tree (algorytm drzewa opinającego)** - określony standardem IEEE 802.1d mechanizm dynamicznego wykrywania i usuwania zapętleń w sieciach zbudowanych przy użyciu tzw. mostów przeźroczystych oraz przełączników ethernetowych (użycie kilku takich urządzeń może spowodować powstanie zapętleń w topologii sieci). Zapętleń takie powodują niepożądane powielanie oraz krążenie ramek w sieci. Algorytm spanning tree zapewnia, że dowolne dwie stacje są połączone tylko jedną ścieżką. Topologia sieci ma kształt drzewa, którego korzeniem jest urządzenie o największym priorytecie (ustalonym przez administratora sieci). Działanie algorytmu oparte jest na periodycznej wymianie, przez wspomniane urządzenia, komunikatów zwanych BPDU (*Bridge Protocol Data Unit*).

**ALOHA** - nazwa popularnego protokołu przypadkowego (rywalizacyjnego) dostępu do medium rozsiewczego (np. radiowego), a także nazwa pierwszej pakietowej sieci radiowej stosującej powyższą metodę dostępu. Dostęp typu ALOHA (bądź S-ALOHA - slotted

ALOHA) zakłada brak koordynacji w pracy stacji ubiegających się o dostęp do medium. W algorytmach typu ALOHA w przypadku zaistnienia kolizji ramek realizowane są różne strategie ich retransmisji. Najprostsza z nich zakłada losowanie momentu retransmisji w ramach określonego przedziału randomizacji, nazywanego też oknem retransmisji. Cechą charakterystyczną sieci stosujących algorytm ALOHA jest możliwość niestabilnej pracy przy dużym obciążeniu kanału.

**analizatory protokołów** - aplikacje (czasem dedykowany sprzęt zainstalowanym oprogramowaniem) rejestrujące przesyłane w sieci bloki danych; prezentujące różnorodne statystyki ruchu oraz analizujące „wychwytywane” bloki (wartości i znaczenie poszczególnych pól pakietów (ramek), związanych z różnymi protokołami komunikacyjnymi).

**analogowy sygnał** - sygnał którego wartość (w przypadku sygnału elektrycznego - wartość napięcia) zmienia się w sposób ciągły. W przeciwieństwie do sygnału analogowego sygnał cyfrowy przyjmuje wartości ze zbioru dyskretnego - najczęściej binarnego (dwie stałe wartości określone najczęściej jako 0 i 1).

**aplikacja zarządzająca przełącznikiem ATM** - integralna część oprogramowania sieci ATM nadzorująca bezkolizyjne i dynamiczne multipleksowanie ścieżek i kanałów wirtualnych w jeden lub kilka strumieni cyfrowych, łączących poszczególne węzły sieci.

**ANSI (American National Standards Institute)** - północnoamerykańska organizacja normalizacyjna skupiająca ok. 300 branżowych komitetów normalizacyjnych współpracujących na zasadzie akredytacji. Komitet zajmujący się telekomunikacją ma symbol T1 i dzieli się na szereg podkomitetów.

**APPC (Advanced Program to Program Communication)** - protokół warstwy sesji w architekturze SAA (*System Application Architecture*) wykorzystywany do współpracy ze stacjami roboczymi w sieci o architekturze SNA. Protokół APPC, wprowadzony na początku lat osiemdziesiątych, zawiera mechanizmy pozwalające na komunikację między aplikacjami pracującymi na różnych systemach, nie angażując systemu komputera centralnego (*mainframe*).

**APPN (Advanced Peer to Peer Networking)** - program realizujący usługi sieciowe typu warstwowego (*peer to peer*) w przypadku równorzędnych komputerów w ramach architektury SNA i korzystający z protokołu APPC. W usługach sieciowych modelu APPN zaimplementowano interfejs API Common Programming Interface for Communications. Mechanizm routingu usług APPN w sesji APPC jest hierarchiczny.

**Archie** - system wyszukiwania informacji na serwerach FTP, dostępny w Internecie. Baza danych Archie zawiera kilka mln nazw programów i zbiorów zgromadzonych na ponad 2 tysiącach publicznych (*anonymous*) serwerach FTP. Od pewnego czasu Archie zastępowane jest przez WWW i przeglądarki webowe.

**architektura logiczna sieci** - zorganizowane w postaci warstw zestawy procedur realizujące ściśle określone funkcje sterujące, komunikacyjne i usługowe, w danej sieci komputerowej. Poszczególne warstwy realizują różne funkcje odpowiedzialne za realizację przekazu danych. Najpopularniejsze architektury to ISO-OSI, TCP/IP, SNA i DNA.

**ARCnet (Attached Resource Computing network)** - sieć LAN o topologii gwiazdy, w której każda stacja robocza jest połączona bezpośrednio z serwerem. Rozwiązań opracowane przez Datapoint Corp. Do celów komunikacji użyto metody dostępu z przesyłaniem znacznika. Standardowa szybkość transmisji 2,5 Mb/s; dostępne są też wersje o szybkości transmisji podwyższonej do 20 Mb/s. Liczba stacji nie przekracza 255.

**ARP (Address Resolution Protocol)** - jeden z protokołów zestawu TCP/IP służący do dynamicznej konwersji adresu IP na adres sprzętowy MAC adaptera sieciowego. Protokół ARP stosowany jest w sieciach lokalnych wspierających sprzętowe rozgłasianie.

**ARPAnet (Advanced Research Project Agency Network)** - rozległa sieć komputerowa łącząca dużą liczbę komputerów obliczeniowych, tzw. hostów. Sieć opracowana i zbudowana w latach siedemdziesiątych na zamówienie amerykańskiego Departamentu Obrony była prototypowym wdrożeniem sieci pakietowej (tzn. sieci z komutacją pakietów). ARPAnet została przekształcona w jądro Internetu. Na podstawie zestawu protokołów sieciowych ARPAnet opracowano protokół IP oraz jeden z najpopularniejszych zestawów protokołów komunikacyjnych TCP/IP, stosowany z powodzeniem nie tylko w Internecie.

**ARQ (Automatic Repeat reQuest)** - technika sterowania przepływem ramek (bloków danych) w sieci wiążąca wykrywanie błędów z automatyczną retransmisją bloków danych. Znanych jest szereg procedur ARQ, wśród których największe znaczenie praktyczne mają metody *Stop-And-Wait* (SAW) oraz metody okienkowe typu *Go-Back-N* (GBN) i z selektywną retransmisją (SR).

**ASCII (American Standards Code for Information Interchange)** - jeden z kilku 7-bitowych kodów transmisyjnych, przyporządkowujący liczbom od 0 do 127 znaki alfanumeryczne i znaki sterujące. Zbiór znaków ASCII jest przeznaczony głównie do wymiany informacji w systemach transmisyjnych i systemach przetwarzania danych. Alfabet ASCII został przyjęty przez CCITT jako międzynarodowy alfabet nr 5. Rozszerzona, 8-bitowa wersja ASCII, przyporządkowuje 256 ciągiem również znaki diakrytyczne i narodowe.

**asynchroniczna transmisja** - sposób transmisji szeregowej, używającej bitów startu i stopu do koordynacji i synchronizacji przepływu znaków danych między urządzeniami końcowymi (modemami).

**ATM (Asynchronous Transfer Mode)** - technika asynchronicznego przekazu danych opracowana z myślą o realizacji usług multimedialnych (przesyłanie glosu, dźwięków, obrazu, danych) i przyjęta jako technika transmisji w szerokopasmowych sieciach B-ISDN. Technika ATM łączy zalety transmisji synchronicznej STM (*Synchronous Transfer Mode*) i transmisji pakietowej, eliminując większość wad tych systemów. Uniwersalność techniki ATM wiąże się z oferowaniem przez nią możliwości: przesyłania stałych porcji informacji o długości 53 bajtów, ustalania indywidualnych przepustowości połączeń gwarantujących dowolne szybkości transmisji w obrębie przyjętych lub istniejących standardów, obsługi transmisji izochronicznych, skalowalności przepływności kanałów i węzłów ATM (zapewniającej możliwość ustalania indywidualnych przepustowości), tworzenia przekazów głównie w trybie połączeniowym, tworzenia wirtualnych połączeń przez sieć zarówno dla pojedynczych kanałów, jak i grup kanałów zwanych ścieżkami wirtualnymi, adaptacji strumienia komórek do dowolnej przepływności medium transportowego, zapewniania „przeźroczystości” przenoszenia informacji przez sieć.

**ATM Forum** - organizacja skupiająca wiele firm telekomunikacyjnych, zajmująca się promocją i nieformalną standaryzacją sprzętu i oprogramowania dla potrzeb ATM.

**BCC (Block Check Character)** - znak lub sekwencja nadmiarowych znaków kontrolnych, generowana przez algorytm kontrolny przed wysłaniem danych łączem transmisyjnym. Urządzenie odbiorcze porównuje odtworzoną sekwencję z sekwencjami dopuszczalnymi, by stwierdzić, czy wystąpiły błędy w transmisji. Wykorzystuje się przy tym następujące metody zabezpieczeń: (1) zabezpieczenia pionowe VRC (*Vertical Redundancy Checking*), polegające na generowaniu bitu parzystości dla każdego znaku danych; (2) kontrolę

wzdłużną LRC (*Longitudinal Redundancy Checking*), polegającą na obliczeniu parzystości dla kolejnych bitów: pierwszego, drugiego itd. - we wszystkich znakach w przesyłanym bloku. Kontrolę LRC łączy się często z VRC realizując tzw. kodowanie iterowane; (3) kontrolę cykliczną CRC (*Cyclic Redundancy Checking*), z użyciem do zabezpieczania danych kodu cyklicznego z generacją ciągu kontrolnego, zwykle 16- lub 32-bitowego.

**bezpieczeństwo sieci komputerowych** - to hasło obejmujące swoim znaczeniem wiele zagadnień związanych z teleinformatyką i dziedzinami pokrewnymi, rozumiane jako całokształt problemów związanych z bezpieczeństwem danych zgromadzonych i przesyłanych w sieci komputerowej. Bezpieczeństwo sieci związane jest nierozerwalnie z efektywnymi systemami kryptograficznymi (DES, RC, RSA, itp.), autoryzacją dostępu, stosowaniem technicznych (specjalizowane serwery separujące sieci tzw. *fire-wall*, oprogramowanie sieciowe z wbudowanymi mechanizmami ochrony), a także nietechnicznych środków ochrony. Problematyka bezpieczeństwa sieci dotyczy też klas zagrożeń związanych z wadami protokołów komunikacyjnych, błędami w oprogramowaniu systemowym, nieprawidłowościemi w pracy administratorów i użytkowników sieci. Identyfikuje również rodzaje naruszeń bezpieczeństwa, w tym kategorie i techniki ataków na sieć.

**B-ISDN** (*Broadband Integrated Services Digital Network*) - sieć szerokopasmowa stanowiąca rozszerzenie wąskopasmowej sieci ISDN. Zgodnie z zaleceniami ITU-T (dawniej CCITT) B-ISDN umożliwia przesyłanie informacji w różnych postaciach: dane, głos, dźwięk jakości CD, zeskanowane obrazy, obrazy video, filmy, sygnały telewizyjne o zwykłej i wysokiej rozdzielczości HDTV. Kanały podstawowe PRI ISDN o szybkości nominalnej 2 Mb/s są łączone przez zwielokrotnienie w trakty szerokopasmowe o przepływności 155 Mb/s, 622 Mb/s, a nawet gigabitowe - zgodnie z przyjętą technologią transmisji. Fizyczny transport danych w łączach szerokopasmowych opiera się zwykle na technice transmisji synchronicznej SDH. Użycie techniki ATM umożliwia efektywne wykorzystanie przepustowości łącz szerokopasmowych przez elastyczne dopasowanie się do przekazów pochodzących ze źródeł o zmiennej szybkości pracy.

**BRI ISDN** (*Basic Rate Interface ISDN*) - jeden z dwóch typów interfejsów cyfrowej sieci abonenckiej ISDN składający się z 2 kanałów typu B (2x64 kb/s) oraz 1 kanału sygnalizacyjnego D (16 kb/s) niezbędnego do nawiązania połączenia i synchronizacji. Łączna przepływność kanału BRI (2B+D16) wynosi 144 kb/s, a po uwzględnieniu synchronizacji, ramkowania i dwukierunkowości przekazów za pomocą tej samej linii - wymagana fizyczna przepływność linii telefonicznej wynosi 192 kb/s. Kanał BRI umożliwia jednoczesną i dwukierunkową pracę dwóch terminali cyfrowych ISDN.

**broadcast** - rodzaj usługi komunikacyjnej polegającej na rozgłaszczeniu informacji. Komunikacja typu broadcast nie określa, gdzie i przez kogo dana usługa zostanie wykonana, a wybór adresata dokonywany jest przez odpowiednie procedury systemowe.

**brouter** - urządzenie komunikacyjne łączące funkcje mostu i routera. Broutera działają jako mosty przy łączeniu sieci o tych samych protokołach względnie jako routery między sieciami o różnych protokołach (np. TCP/IP i X.25), realizując dodatkowo funkcje routerów dokonując np. wyboru tras. Wypierane są obecnie przez routery wieloprotoakołowe.

**BSC** (*Binary Synchronous Communication*) - synchroniczny, znakowy protokół komunikacyjny opracowany przez IBM i przeznaczony do pracy wsadowej między komputerami mainframe a zdalnymi terminalami, nazywany też BISYNC. Działa z zestawem znaków ASCII i EBCDIC; obecnie wyparty przez protokoły SDLC i HDLC, oferujące większe możliwości komunikacyjne.

**BUS** (*Broadcast Unknown Server*) - wielozadaniowy serwer, definiowany w standardzie LANE, służący do transmisji pakietów o nieznanym adresie przeznaczenia oraz umożliwiający rozgłaszczenie danych, przesyłanie danych do grupy użytkowników jak też obsługę zapytań o nieznane adresy, w ramach jednej emulowanej sieci.

**CAC** (*Connection/Call Acceptance Control*) - funkcja sterowania (w sieci ATM) przyjmowaniem wywołań, definiowana jako zespół działań mających na celu podjęcie decyzji o przyjęciu/odrzuceniu nowego wywołania, a w przypadku jego przyjęcia - przydzielenie odpowiednich zasobów sieci, pozwalających na realizację połączenia o określonej jakości.

**CBR** (*Constant Bit Rate*) - usługa (w sieci ATM) o stałej szybkości bitowej - opracowana dla źródeł ruchu wymagających stałej szybkości transmisji w czasie trwania połączenia. W przypadku tej kategorii usług wartość wymaganego pasma transmisyjnego określana jest przez maksymalną szybkość przekazu PCR. Kategoria ta jest wykorzystywana do emulacji łącz cyfrowego o przepływności 2.048 Mb/s. Przykładami aplikacji korzystających z tej usługi są interaktywne przekazy mowy czy też transmisje sygnałów wideo w standardzie MPEG1;

**CCIR** (*International Consultative Committee on Radio*) - komitet doradczy ITU (agendy ONZ), zajmujący się opracowywaniem zaleceń i standardów w komunikacji radiowej.

**CCITT** (ang. *International Consultative Committee on Telephony & Telegraphy*) - komitet doradczy i konsultacyjny ITU (agendy ONZ), zajmujący się opracowaniem i aktualizacją (co 4 lata) zaleceń i standardów telekomunikacyjnych (standardy Vxx). Od 1993 r. nosi nazwę ITU-T.

**CEPT** (*The European Conference of Posts and Telecommunications*) - stowarzyszenie koordynujące działalność 26 europejskich instytucji i krajowych administracji pocztowo-telekomunikacyjnych. Koordynuje działalność operatorów sieci telekomunikacyjnych. Zajmuje się także standaryzacją łącz międzynarodowych w krajach związanych z EWG. W 1988 r. ze stowarzyszenia został wydzielony instytut normalizacyjny ETSI, zajmujący się standaryzacją w obrębie telekomunikacji.

**CIR** (*Committed Information Rate*) - wskaźnik przydziału pasma komunikacyjnego, stosowany w sieciach Frame Relay, do określenia zajętości kanału transmisyjnego lub wirtualnego. Wielkość wskaźnika jest wstępnie negocjowana między użytkownikiem a usługodawcą i nie powinna ulegać zmianie w trakcie sesji połączeniowej. Sumaryczna wartość wynegocjowanych wskaźników CIR, dla różnych usług i abonentów korzystających z tego samego kanału transmisyjnego, nie może przekroczyć unormowanej dostępnej średniej szybkości transmisji oferowanej przez dane medium transmisyjne. CIR ma zawsze wartość mniejszą od jedności lub co najwyżej 100% binarnej przepływności kanału (w tym wirtualnego); CIR wyrażany jest zwykle nieformalnie wielokrotnością przepływności 64 kb/s.

**CMIP** (*Common Management Information Protocol*) - protokół zarządzania siecią oparty na modelu OSI przydatny do współpracy z publiczną, komutowaną siecią telefoniczną.

**CRC** (*Cyclic Redundancy Checking*) - metoda zabezpieczania danych kodem cyklicznym; również metoda określania poprawności transmisji cyfrowej w łączu telekomunikacyjnym. Przy zabezpieczeniu typu CRC blok informacyjny traktuje się jako wielomian, który w nadajniku dzieli się modulo 2 przez specjalny wielomian generujący CRC. W przypadku zabezpieczeń stosowanych w sieciach publicznych jest to zwykłe wielomian szesnastego stopnia (CCITT zaleca kilka wersji wielomianu generującego, popularnym jest  $x^{16} + x^{12} + x^5 + 1$ ). Otrzymana reszta tworzy 16-bitową sekwencję kontrolną FCS transmitowaną na końcu bloku. W odbiorниku odebrany blok informacyjny jest również

dzielony przez taki sam wielomian. Transmisja danych jest uznana za poprawną wtedy i tylko wtedy, gdy reszta z dzielenia, otrzymana w dekoderze, jest identyczna z sekwencją FCS. Brak zgodności obu sekwencji wymusza przesłanie odpowiedniej informacji kanałem sprężenia zwoрtnego i retransmisję błędnych bloków.

**CSMA** (*Carrier Sense Multiple Access*), **CSMA/CA** (*Collision Avoidance*), **CSMA/CD** (*Carrier Sense*) - metody dostępu do medium związane z wykrywaniem nośnej w kanale poprzez prowadzenie nasłuchu kanału. Transmisja ramki jest możliwa tylko wtedy, gdy w kanale nie jest prowadzona inna transmisja. W celu ograniczenia liczby konfliktów (które mogą zaistnieć z uwagi na skończone opóźnienia propagacyjne w medium) w sieciach LAN stosuje się jedną z dwóch procedur dostępu: unikania kolizji CSMA/CA lub wykrywanie kolizji CSMA/CD. W metodzie CSMA/CA, proponowanej w bezprzewodowej sieci LAN standardu 802.11, każda stacja użytkownika przed rozpoczęciem nadawania prowadzi nasłuch łączą i po stwierdzeniu ciszy sygnalizuje krótką ramką swój zamiar zgłoszenia chęci nadawania RTS (*Request To Send*), a następnie, po oczekaniu (lub odbiorze stosownego potwierdzenia CTS (*Clear To Send*)) transmituje swoją ramkę danych. Pozostałe stacje po stwierdzeniu zgłoszenia przechodzą w stan oczekiwania na sygnał końca ramki. W przypadku kolizji, o dostęp do medium mogą ubiegać się tylko stacje, które ją spowodowały; każda z innym, losowo ustalanym opóźnieniem. W dostępie z wykrywaniem kolizji CSMA/CD (*Collision Detection*), podstawowej metodzie dostępu realizowanej w sieciach lokalnych opisanych standardem IEEE 802.3 (w tym Ethernet), stacja przystępująca do nadawania również czeka na ciszę w medium, a po jej detekcji wysyła swoje dane, nie przerywając jednak nasłuchu łączą. Stacja, która pierwsza wykryje ewentualną kolizję, przerwa transmisję pakietu i generuje tzw. *jamming signal*. Wszystkie uczestniczące stacje również przerwyają nadawanie na losowo wybrany okres, po którym transmisję wznowią stacja o najkrótszym okresie przerwy w nadawaniu.

**datagram** - wiadomość (lub blok danych) przesyłana przez sieć komunikacyjną między komputerami lub abonentami sieci, bez uprzedniego zestawienia połączenia logicznego między obiektami warstwy sieciowej modelu OSI. Usługa datagrowa realizowana jest zgodnie z trybem bezpołączeniowym; nie daje ona zatem gwarancji doręczenia pakietów do adresata; możliwy jest też odbiór pakietów w innej kolejności, niż zostały one nadane.

**DCE** (*Data Circuit terminating Equipment lub Data Communication Equipment*) - w komunikacji sieciowej jest to dowolne urządzenie łączące komputer lub terminal z kanałem komunikacyjnym lub siecią publiczną; zwykle oznacza modem lub konwerter sygnałów. Komunikuje się z DTE.

**DDCMP** (*Digital Data Communications Message Protocol*) - zorientowany znakowo protokół warstwy łączą danych opracowany przez firmę DEC z przeznaczeniem dla szerokiego zestawu sieci komputerowych (sieci synchroniczne i asynchroniczne, z kanałami dedykowanymi lub komutowanymi, pracującymi w trybie półduplekowym bądź duplekowym, z połączeniami typu punkt-punkt względnie punkt-wielopunkt). DDCMP może też współpracować z interfejsami przystosowanymi do transmisji szeregowej bądź równoległej.

**DECnet** (*Digital Equipment Corporation network*) - nazwa sieci służącej do integracji sieci lokalnych grupujących komputery firmy DEC (*Digital Equipment Corporation*), od największych komputerów typu mainframe do osobistych klasy PC. Atutem sieci/protokołu DECnet jest możliwość pracy pod nadzorem różnych systemów operacyjnych: VMS, DOS, Ultrix (DEC-Unix); wadą jest ograniczona adresacja komputerów oraz współpraca z komputerami tylko jednego producenta.

**deskryptory źródła** - są to podstawowe parametry, wykorzystywane w sieci ATM do opisu charakterystyk pracy źródła. Najważniejsze znaczenie, z punktu widzenia możliwości zawarcia kontraktu ruchowego oraz implementacji prewencyjnej metody sterowania ruchem w sieci ATM mają: (1) wartość maksymalna szybkości generowania komórek PCR (*Peak Cell Rate*) - definiowana jako odwrotność minimalnego odstępu czasu między kolejnymi komórkami generowanymi przez źródło; (2) graniczna wartość średniej szybkości transmisji komórek SCR (*Sustainable Cell Rate*); (3) maksymalny rozmiar paczki komórek MBS (*Maximum Burst Size*) - określany w przypadku, gdy źródło transmituje komórki z szybkością równą SCR;

**DNA** (*Digital Network Architecture*) - architektura sieciowa opracowana na potrzeby firmy DEC i stosowana głównie w sieciach DECnet. Faza V implementacji architektury DNA zakłada możliwość pełnej współpracy protokołów DNA z protokołami ISO-OSI.

**DNS** (*Domain Name System*) - instalowany zwykle na dedykowanym serwerze sieciowym system adresowania dokonujący konwersji numerycznych adresów internetowych (32 bity w IPv4 lub 128 w wersji rozszerzonej - IPv6) na łańcuchy nazw składających się z wyrazów lub mnemoników określających nazwy użytkowników i ich lokalizacje. Zwykle instalowany na dedykowanym serwerze sieciowym.

**domena** - zbiór węzłów (stacji) sieciowych, które tworzą jednostkę administracyjną. Podział na domeny ma na celu uproszczenie zarządzania siecią. Każdy węzeł sieciowy należy do co najmniej jednej domeny.

**domena kolizyjna** - wszystkie połączone ze sobą węzły sieciowe, które wykorzystują wspólne medium oraz zdcentralizowane (rozproszone) mechanizmy transmisji oparte na rywalizacji o dostęp (np. CSMA/CD) do tego medium. Domeną kolizyjną jest na przykład sieć Ethernet wykorzystująca koncentratory nazywane powszechnie hubami (każda stacja podłączona do huba ma bezpośredni wpływ na możliwości transmisji innych stacji). Domena kolizyjna jest logicznym odpowiednikiem segmentu sieci lub połączonych regeneratorami kilku segmentów.

**domena rozgłoszeniowa** - zbiór węzłów i domen kolizyjnych, do których docierają ramki MAC kierowane do nieznanego adresatów i ramki adresowane „do wszystkich”. Domene rozgłoszeniową tworzą przykładowo wszystkie węzły sieci lokalnej podłączone do jednego portu routera (sieć taka może być zbudowana w oparciu o urządzenia działające w drugiej warstwie modelu OSI, które nie filtrują ramek rozgłoszeniowych, takie jak mosty czy proste przełączniki ethernetowe).

**DQDB** (*Distributed Queue Dual Bus*) - standardowe rozwiązanie (IEEE 802.6) opracowane dla sieci MAN (1990 r.), oparte na dwóch magistralach światłowodowych prowadzących transmisje w przeciwnych kierunkach i cyklicznym generowaniu w stacjach końcowych magistral ciągów ramek, nazywanych szczelinami czasowymi (każda o długości 53 bajtów), w których stacje umieszczają swoje 52-bajtowe bloki danych. Stacje uzyskują dostęp do szczelin czasowych zgodnie ze zgłoszonym przez nie zapotrzebowaniem (realizowanym na zasadzie rozproszonej rezerwacji). Dla obsługi transmisji izochronicznych, wymagających stałego pasma (przesyłanie głosu, dźwięku, obrazu), stacje uzyskują cykliczny dostęp do szczelin, zapewniający realizację aplikacji czasu rzeczywistego. Jednoczesna i niezależna transmisja w dwóch przeciwbieżących magistralach umożliwia duplekowy tryb pracy, dzięki czemu sieć DQDB ma podwojoną zdolność transmisyjną (nawet do 600 Mb/s). Topologia sieci DQDB może być dynamicznie rekonfigurowana ze struktury magistralowej w strukturę przypominającą pierścień i odwrotnie. W strukturze pierścieniowej jedna stacja generuje wieloramki w obu magistralach. Fizyczne lub logiczne uszko-

dzenie dwumagistralowej struktury pierścieniowej przekształca automatycznie sieć DQDB w dwa otwarte pierścienie, bez zmiany protokołów i zasad sterowania, oraz zezwala na kontynuowanie transmisji po przerwie niezbędnej na rekonfigurację sieci.

**DTE** (*Data Terminal Equipment*) - terminal teleinformatyczny, wykorzystujący do transmisji publiczną sieć telekomunikacyjną PSTN. DTE komunikuje się bezpośrednio z systemem DCE stanowiącym zakofczenie sieciowe nadzorowane przez operatora sieci publicznej.

**dupleks (duplex)** - dwukierunkowy i jednoczesny przekaz danych, realizowany zwykle w postaci asynchronicznej transmisji szeregowej przez jeden kanał transmisyjny. Praca w trybie pełnduplekowym, przy wyższych szybkościach transmisji z zastosowaniem modemów wymaga stosowania rozbudowanych układów kompensacji echa.

**EARN** (*European Academic and Research Network*) - rozległa sieć komputerowa łącząca europejskie ośrodki akademickie; część sieci BITNET, współpracująca z innymi sieciami rozległymi, np. Internetem.

**EBCDIC** (*Extended Binary Coded Decimal Interchange Code*) - kod 8-bitowy wykorzystywany do reprezentacji zestawu znaków powszechnie stosowanych w dużych komputerach typu mainframe zarówno firmy IBM, jak i innych producentów. W przeciwieństwie do zestawu znaków ASCII, położenie liter alfabetu w zestawie 256 znaków EBCID nie jest „ciągłe”. Nie ma też bezpośredniego odpowiednika wszystkich znaków zestawu EBCID w ASCII (i na odwrót). W komputerach osobistych PC i terminalach sieciowych opartych na tych komputerach kod EBCID został wyparty przez ASCII.

**EIA** (*Electronic Industry Association*) - amerykańskie Stowarzyszenie Przemysłu Elektronicznego definiujące wiele standardów telekomunikacyjnych, przyjmowanych później przez międzynarodowe organizacje standaryzacyjne. Najbardziej znany jest standard EIA 232 określający parametry techniczne połączenia (styk) między modemem, a publiczną siecią telekomunikacyjną PSTN. W Europie styk ten jest znany w wielu odmianach pod nazwą RS 232.

**enkapulacja lub kapsułkowanie (encapsulation)** - mechanizm przesyłania danych jednego protokołu poprzez sieć pracującą pod kontrolą innego, równorzędnego (w znaczeniu modelu OSI) protokołu komunikacyjnego (np. Ethernet i FDDI, IPX i IP). Kapsułkowanie jest stosowane w sytuacjach, gdy niemożliwa jest (z powodu różnic pomiędzy protokołami bądź ograniczeń sprzętowych) konwersja postaci ramek z jednego protokołu na drugi. Przykładowo ramki ethernetowe, które są wymieniane pomiędzy sieciami Ethernet połączonymi poprzez sieć FDDI, są na czas transmisji siecią sprzągającą w całości „za-kapsułkowane” wewnętrz ramki FDDI. Kapsułkowanie jest przeźroczyste dla komunikujących się stacji i jest realizowane przez urządzenia sprzągające sieci pracujące pod kontrolą różnych (tu: kapsułkowanych) protokołów. Funkcję „kapsułkowania” pakietów wykonują głównie routery, a także mosty stanowiące węzły sieci heterogenicznych. W miejscu przeznaczenia dokonywana jest operacja odwrotna, przywracająca pierwotną postać pakietu (ramki).

**Ethernet** - najpopularniejsze rozwiązanie sieci LAN opracowane przez firmę Xerox Corporation (1975 r.) i rozwijane przez Digital Equipment oraz Intel. Sieci Ethernet znormalizowane przez IEEE (przyjęcie standardu 802.3), pracują najczęściej z przepływnością 10 Mb/s (generalnie od 1 do 20 Mb/s) z wykorzystaniem dostępu typu CSMA/CD. Podstawowym medium transmisyjnym jest kabel współosiowy (10Base-2 lub 10Base-5) konfigurowany w postaci magistrali, do której można podłączyć maksymalnie 8 tys. stacji roboczych. Możliwe jest przystosowanie innych mediów (skrętka, światłowód) i stosowanie innych topologii. Maks. zasięg sieci Ethernet wynosi 2500 m (lub 4600 m w przypadku

kabli światłowodowych). Nowsze rozwiązania technologiczne umożliwiają szybkość transmisji 100 Mb/s - w sieciach typu Fast Ethernet (IEEE 802.3u), bądź 1 Gb/s - w sieci Gigabit Ethernet (IEEE 802.3z).

**Ethernet 100 Mb/s (Fast Ethernet)** - sieć lokalna pracująca z szybkością 100 Mb/s, będąca rozwinięciem wcześniejszego standardu sieci komputerowych Ethernet (10 Mb/s). Standard szybkiego Ethernetu realizowany jest w instalacjach 100Base-T (zgodnie z terminologią IEEE ma on oznaczenie 802.3u). Technologia opracowana jest głównie z myślą o sieciach o topologii gwiaździstej z wykorzystaniem hubów lub przełączników. Istotnym ograniczeniem, w porównaniu z klasycznymi sieciami 10BaseT, podlega rozmiar sieci. Maksymalna odległość stacji od przełącznika zostaje zmniejszona do 100 m. (dla skrótki).

**ETSI** (*European Telecommunications Standard Institute*) - Europejski Instytut Standardów Telekomunikacyjnych utworzony z inicjatywy EWG w celu standaryzacji produktów telekomunikacyjnych w zakresie sprzętu, sieci i usług komunikacyjnych. Przygotowywaniem projektów norm zajmuje się 12 branżowych komitetów technicznych, dzielących się na podkomitety i zespoły robocze.

**FC (Feedback Control)** - mechanizm sterowania (w sieci ATM) przepływem ze sprzężeniem zwotnym, definiowany jako zbiór działań podejmowanych przez sieć i adresata danych, w celu wpływu na szybkość generowania komórek przez źródło (w zależności od stanu sieci). Mechanizm ten wykorzystuje tzw. powiadomienie w przód - bit EFCI (*Explicit Forward Congestion Indicator*) w nagłówku komórki - do poinformowania źródła o przeciążeniu w sieci.

**FD (Frame Discard)** - funkcja odrzucania ramek (w sieci ATM) umożliwiająca odrzucanie całych ramek w przypadku przeciążenia sieci i chroniąca tym samym pozostałe ramki przed skutkami powstałe w sieci przeciążenia.

**FDDI (Fiber Distributed Data Interface)** - popularne, standardowe (standard ANSI X.3.T.9.5) rozwiązanie szybkiej światłowodowej sieci cyfrowej o topologii podwójnego pierścienia. Dane są przesyłane z szybkością 100 Mb/s, natomiast rzeczywista szybkość transmisji w pierścieniu wynosi 125 MBodów. Wynika to z zastosowania kodu transmisyjnego 4B/5B. Technologia FDDI znajduje zastosowanie w instalacjach sieci lokalnych i metropolitanálnych, głównie przyłączeniu sieci LAN. Jako medium transmisyjne stosuje się światłowody jedno- lub wielomodowe. Od niedawna jest też możliwa realizacja sieci FDDI za pomocą kabli miedzianych, realizowanych za pomocą nieekranowanej skrętki UTP kategorii 5, według specyfikacji TP-PMD. W sieciach FDDI stosuje się metodę dostępu polegającą na przekazywaniu tokenu (znacznika), podobną do stosowanej w sieci Token Ring. Istnieje możliwość nadawania różnych priorytetów przesyłanym danym, a także dokonywania rezerwacji tokena (*restricted token*), w przypadku wymiany między parami stacji dużych zbiorów danych. W sieci nie występują stany zablokowania, bądź niesprawiedliwego „zawłaszczenia” medium, gdyż natychmiast po nadaniu komunikatu stacja musi wysłać pusty token, który może być przejęty przez inną stację. W sieci możliwe jest krażenie wielu ramek kontrolowanych przez administratora (kontroli podlega wielkość, liczbę i częstotliwość przesyłania ramek). Wysoka niezawodność pracy sieci FDDI wiąże się z tokenową metodą dostępu, co w połączeniu z dużą szybkością (100 Mb/s), konfigurowaniem wielu (nawet do 1000) stacji oraz topologią podwójnej pętli o zasięgu do 200 km czyni tę technologię przydatną do budowy korporacyjnych i metropolitanálnych sieci szkieletowych.

**FDDI-II** - nowsza wersja sieci FDDI, przeznaczona dla zastosowań multimedialnych, wymagających stałego opóźnienia w dostępie do medium. W tej wersji całe pasmo transmisyjne

sieci (100 Mb/s) jest dzielone na 16 kanałów szerokopasmowych o przepustowości 6,144 Mb/s każdy, zajmujących łącznie pasmo o przepływności 99,072 Mb/s. Kanały 6,144 Mb/s mogą być agregowane lub dzielone na podkanały po 64 kb/s każdy, zapewniając podział logiczny pełnego pasma 100 Mb/s na kanały o praktycznie dowolnej przepływności. Pozostała część przepustowości sieci, tj. 928 kb/s, jest wykorzystywana zgodnie z zasadami obowiązującymi w FDDI. Łączenie podkanałów polega przy tym na multiplesacji czasowej, związanej z przydziałem użytkownikowi ustalonej liczby szczelin czasowych dla realizacji jego transmisji izochronicznych. Do tego celu w sieci FDDI-II używany jest nowy typ protokołu komunikacyjnego HRC (*Hybrid Ring Control*), zapewniający transmisję danych w trybie połączonym (dla usług multimedialnych).

**Frame Relay (FR)** - protokół i szybka sieć pakietowa stosowana w szybkich cyfrowych sieciach publicznych lub prywatnych. Protokół Frame Relay specyfikuje zasady współpracy stacji w obrębie dwóch dolnych warstw modelu ISO-OSI. Sieć transmisyjna z przełączaniem ramek FR funkcjonuje na łączach cyfrowych wysokiej jakości, zwykle światłowodowych, o niskiej stopniu błędów i zmiennej przepływności w zakresie od 56 kb/s do 45 Mb/s. Sieć FR zastępuje z powodzeniem sieci pakietowe z protokołem X.25, o znacznie niższych przepływnościach, niższej jakości transmisji, oferując większą niezawodność i elastyczne wykorzystanie istniejących zasobów sieci pakietowych PSDN.

**FTP (File Transfer Protocol)** - usługa przesyłania zbiorów (plików), o dowolnej wielkości, pomiędzy dwiema stacjami sieci Internet. Protokół zapewnia kontrolę poprawności transmisji oraz praw dostępu do danych. Do uzyskania dostępu do odlegiej stacji służy identyfikator użytkownika oraz hasło. Dostępne są również zbiory na serwerach publicznych (anonymous) FTP, dla których identyfikatorem jest słowo „anonymous”, a hasłem - dla statystyki - identyfikator użytkownika.

**GAN (Global Area Network)** - sieć globalna łącząca heterogeniczne sieci komputerowe o międzynarodowym zasięgu. W sieciach GAN stosowane są różnorodne protokoły komunikacyjne i media transmisyjne. Przykładami tego typu sieci są: Internet, EARN, BITNET.

**Gigabit Ethernet** (Ethernet 1000 Mb/s) - szybka sieć LAN o przepływności 1 Gb/s, stanowiąca najnowszą wersję standardu Ethernet (oznaczaną symbolem IEEE 802.3z). W sieci Gigabit Ethernet zastosowano ten sam format ramki i sposób dostępu do medium jak w zwykłym Etherencie 10 Mb/s. Sieć jest przeznaczona głównie do realizacji światłowodowych połączeń serwerów i superserwerów z szybkimi przełącznikami sieciowymi. Efektywne wykorzystanie przepustowości wymaga stosowania najnowszych przełączników filtrujących pakiety z szybkością 1 mln pakietów na sekundę - wyposażonych w agentów SNMP do zarządzania oraz realizujących algorytm Spanning Tree, pozwalający na tworzenie łączys zapasowych i eliminację pętli. Instalacja kart 1 Gb/s w komputerach PC, nawet najwyższej klasy, może okresowo całkowicie zablokować działanie systemu operacyjnego. Zachowanie protokołu CSMA/CD i typowych rozmiarów ramek Ethernetu istotnie ogranicza rozmiary sieci Gigabit Ethernet.

**gniazdo** - interfejs programowy umożliwiający aplikacjom dostęp do protokołów TCP i UDP i wymianę danych poprzez sieć pracującą pod kontrolą protokołów TCP/IP.

**grupowa transmisja pakietów (multicast transmission)** - transmisja, w której odbiorcą jest grupa węzłów. Przynależność węzła do danej grupy może zmieniać się w sposób dynamiczny (w trakcie transmisji).

**Gopher** (modyfikacja zwrotu Go for it) - środowisko ponad 3000 aktualnie włączonych serwerów systemu Gopher dostępnych w sieci Internet. Serwery Gopher udostępniają

informacje według hierarchicznego menu z ograniczeniem do prezentacji zbiorów tekstowych w postaci spisu publikacji, treści, wykazów, adresów itp. Zbiory niedostępne na wybranym serwerze są automatycznie wyszukiwane na innych i łączone z oddzielnymi dokumentami znajdującymi się w różnych serwerach systemu Gopher. W trakcie poszukiwań system realizuje: przesyłanie plików, zmianę katalogów, rejestrację w komputerach za pomocą programu Telnet, oraz zasięga informacji w innych serwerach: Archie i WAIS. Centralny serwer systemu Gopher jest zlokalizowany na Uniwersytecie Minnesota pod adresem: gopher.micro.umn.edu.

**HDLC (High Level Data Link Control)** - zorientowany bitowo protokół transmisyjny warsztaty łączące danych opracowany przez ISO dla modelu odniesienia OSI. HDLC umożliwia transfer ramek w trybie pełnodupleksowym lub półdupleksowym, w połączeniach punkt-punkt lub wielopunktowych. Podzbioru HDLC są stosowane do sygnalizacji i kontroli pracy łączys w sieciach X.25, ISDN i Frame Relay.

**HIPERLAN (High Performance Radio LAN)** - opracowany przez ETSI standard bezprzewodowej sieci lokalnej WLAN, pozwalający na realizację transmisji do 20 Mb/s przy zasięgu ok. 50 m. HIPERLAN pozwala też na rozszerzenie zasięgu działania do 800 m jednakże z ograniczeniem przepływności do 1 Mb/s. Dla sieci HIPERLAN, działającej zwykle w pomieszczeniach zamkniętych, ustaloną dla Europy dwa przedziały częstotliwości: 5,15-5,30 GHz i 17,1-17,3 GHz. W paśmie 5 GHz zdefiniowano 5 kanałów o szerokości 25 MHz każdy, z dwoma zewnętrznymi pasmami ochronnymi po 12,5 MHz. Możliwe są dwa tryby pracy sieci HIPERLAN: dopuszczający transmisję wieloetapową oraz improwizowany (doraźny - ad hoc) ustalający bezpośrednie połączenia między komputerami PC (stacjonarnymi i przenośnymi) znajdującymi się w jednym pomieszczeniu. Dostęp do medium w sieci HIPERLAN realizowany jest zgodnie z zasadą NPMA (*Non-preemptive Priority Multiple Access*) dopuszczającą rywalizację w obrębie zgłoszeń o zadanym priorytecie. Pięć poziomów, dynamicznie modyfikowanych priorytetów pozwala na skuteczną eliminację kolizji ramek i zapewnia przy dużych obciążeniach sieci prawdopodobieństwo kolizji mniejsze od 0,035.

**homogeniczna sieć** - jednorodna sieć komputerowa łącząca komputery, o podobnej architekturze, pochodzące od jednego producenta; zwykle sieć zarządzana tym samym systemem operacyjnym.

**hub** - centralne urządzenie komunikacyjne pełniące funkcje koncentratora w sieciach lokalnych o topologii gwiazdy. Początkowo hub pełnił rolę prostego pasywnego rozgałęźnika w sieciach Ethernet o medium skrętkowym (10Base-T). Obecnie stosuje się huby aktywne (wzmacniające sygnały), inteligentne (zarządzane protokołem SNMP), huby obsługujące różne media transmisyjne (skrętkę, koncentryk, światłowód), a także huby przełączające (zwane czasem przełącznikami LAN bądź przełącznikami ethernetowymi).

**IEC (International Electrotechnical Commission)** - Międzynarodowy Komitet Elektrotechniczny, wydzielony z ISO, wyspecjalizowany w zakresie elektryki, elektroniki i telekomunikacji; koordynuje prace wielu organizacji normalizacyjnych, współpracuje głównie z ISO, ITU, CCITT, CCIR.

**IEEE (Institute of Electrical and Electronic Engineers)** - amerykańskie stowarzyszenie zawodowe inżynierów elektryków i elektroników działające na rzecz standardów. Efektem prac IEEE jest opracowanie kilku istotnych standardów sieciowych serii IEEE 802.x na potrzeby telekomunikacji, wśród których najpopularniejsze i najważniejsze to:

- **IEEE 802.2** - standard definiujący zasady sterowania przepływem ramek w sieciach LAN; w znacznym stopniu oparty na protokole HDLC,

- **IEEE 802.3** - traktowany zwykle jako standard sieci Ethernet 10Mb/s, specyfikujący procedury działania sieci, w tym metodę dostępu CSMA/CD, zasady współdzielenia pasma, sygnalizację w sieci; dodatkowo definiujący też standard Fast Ethernet (IEEE 802.3u) oraz Gigabit Ethernet (IEEE 802.3z).
- **IEEE 802.4** - standard dla lokalnych magistralowych sieci przemysłowych, z dostępem opartym na mechanizmie tokenowym, z zastosowaniem 75 ohmowych kabli koncentrycznych (CATV) lub światłowodowych,
- **IEEE 802.5** - standard dla sieci pętlowej Token Ring wspieranej przez IBM, o szybkości transmisji 4 lub 16 Mb/s, a obejmujący: okablowanie skrętkowe UTP/STP, dostęp tokenowy, topologie i metody łączenia sieci Token Ring.
- **IEEE 802.6** - standard dla sieci metropolitalnych MAN (algorytm dostępu DQDB).

Należy podkreślić, że normy IEEE są adaptowane przez ISO (8802.x).

**IETF (Internet Engineering Task Force)** - grupa zespołów roboczych Internetu opracowująca protokoły i standardy współpracy sieciowej, prezentowane w postaci zaleceń RFC (*Request For Comments*).

**internet** - ogólnie przyjęte określenie wielu połączonych ze sobą sieci komputerowych.

**Internet** (internet pisany z dużej litery) - globalna sieć komputerowa korzystająca z zestawu protokołów TCP/IP, łącząca rozsiane po świecie lokalne komputery firm i instytucji edukacyjnych, badawczych, rządowych, przemysłowych oraz prywatnych, a także serwery WWW.

**intersiec** - sieć komputerowa składająca się z wielu połączonych ze sobą sieci homobądź heterogenicznych. Integralną częścią intersieci są węzły (routery, huby), łączące poszczególne sieci i segmenty ze sobą i pełniące rolę urządzeń kierujących ruchem pakietów między sieciami. W intersieci każda sieć (podsieć) musi mieć swój indywidualny adres, a w konkretnej sieci - odpowiedni adres musi posiadać również każda stacja sieciowa.

**intranet** - nowe rozwiązanie funkcji sieci Internet, odnoszące się do sieci LAN i obejmujące zasięgiem ograniczony obszar (biuro, pojedynczy zakład, grupę przedsiębiorstw). Elementy intranetu obejmują: sieć LAN (lub najwyższej MAN), prywatne serwery webowe, serwery zakładowe i ewentualnie komputer mainframe połączone z siecią Internet z zastosowaniem dodatkowej separacji w postaci tzw. zapory ogniowej (*firewall*). Istotą intranetu są prywatne serwery webowe i lokalne przeglądarki (browsery), współpracujące ze sobą za pomocą protokołu komunikacyjnego TCP/IP w obrębie sieci lokalnej.

**IPoverATM** - standard opisujący zasady wspomagania protokołu IP przez sieć ATM; w szczególności określający zasady konwersji adresów IP na adresy ATM oraz zasady realizacji połączeń wirtualnych; umożliwiający przesyłanie datagramów IP, a także metody rozmawiania datagramów IP w sieci ATM.

**IP switching** - najnowsza technologia przełączania w sieciach TCP/IP, łącząca zapożyczoną z ATM technikę szybkiego przełączania z funkcją routingu, wymaganą przy przesyłaniu informacji przez kanały wirtualne Internetu. Technologia IP switching wyróżnia się spośród innych znanych technik przełączania wirtualnego specjalnymi mechanizmami programowymi, zapewniającymi połączenie adresów IP warstwy trzeciej z adresami fizycznymi MAC, związanymi z warstwą drugą. Dzięki temu transport danych może być ponad dwudziestokrotnie szybszy (kilka milionów pakietów na sekundę) niż uzyskiwany do tej pory za pomocą wieloprotokółowych routerów, stosujących klasyczne protokoły routingu RIP (*Routing Information Protocol*) oraz OSPF (*Open Shortest Path First*).

**IPX (Internet Packet eXchange)** - podstawowy warstwowy protokół komunikacyjny stosowany w sieciach lokalnych NetWare System. Zapewnia realizację usług w sieciowym systemie operacyjnym NetWare dla architektury klient/servwer. IPX jest protokołem datagramowym, przesyłającym dane w trybie bezpołączeniowym. Rozszerzenie o wersję protokołu połączeniowego IPX/SPX (*Sequenced Packet eXchange*) umożliwia obsługę ramek o zmiennej wielkości przesyłanych w trybie „monopolizującym”, z przeznaczeniem do obsługi dużych pakietów (całych plików) danych. Zmodernizowana powłoka stacji roboczych automatycznie wyszukuje alternatywne drogi przez sieć w przypadku uszkodzenia tras. IPX jest zastępowany stopniowo (od 1996 r.) przez APC (*Advanced Core Protocol*).

**ISO (International Standards Organization)** - międzynarodowa organizacja standaryzacyjna, zrzeszająca krajowe organizacje normalizacyjne (72 państwa członkowskie i 17 członków korespondentów). Zajmuje się normalizacją wszystkich dziedzin techniki, z wyjątkiem elektryki, elektroniki i telekomunikacji, pozostających w gestii wyspecjalizowanej komisji IEC. Wprowadza standardy o charakterze globalnym.

**IsoEthernet** - standardowe rozwiązanie multimedialnej sieci LAN (standard 802.9) oferujące realizację aplikacji czasu rzeczywistego w sieci o topologii drzewiastej z wykorzystaniem skrętek UTP. W standardzie 802.9 kluczową rolę pełni specjalizowany hub zarządzający pracą stacji końcowych. Zaimplementowany w nim algorytm autonegoacji pozwala na ustalenie jednego z trzech trybów pracy stacji przyłączonych do huba: wielousługowego, izochronicznego i podstawowego. W dwóch pierwszych trybach pracy w kanale hub-stacja definiowana jest wieloramka TDMA z 256 szczelinami czasowymi, pozwalającymi na przesyłanie w sposób izochroniczny bądź asynchroniczny poszczególnych bajtów danych. W trybie izochronicznym cała przepustowość kanału równa 15.872 Mb/s wykorzystywana jest do obsługi aplikacji multimedialnych. W trybie wielousługowym w ramce TDMA definiuje się 5 typów szczelin tworzących kanały: P o przepustowości 10 Mb/s (do obsługi ruchu asynchronicznego w ramach standardu IEEE 802.3), C o łącznej przepustowości 6.144 Mb/s (kanal typu C składa się z 96 ISDNowskich kanałów typu B), D o przepustowości 64 kb/s, M o przepustowości 96 kb/s oraz kanału synchronizacji o przepustowości 64 kb/s. W trybie podstawowym kanał jest wykorzystywany do wymiany ramek przesyłanych z szybkością 10 Mb/s, zgodnie z metodą CSMA/CD, charakterystyczną dla standardu IEEE 802.3 (rozwiązanie 10Base-T).

**ITU (International Telecommunication Union)** - Międzynarodowa Unia Telekomunikacyjna; najstarsza i jednocześnie o najszerszym terytorialnie zakresie działania organizacja międzynarodowa (agenda ONZ), w której poszczególne kraje są reprezentowane przez 174 krajowe administracje łączności. Członkami wspierającymi są także: operatorzy telekomunikacyjni, producenci i dostawcy sprzętu oraz inne organizacje międzynarodowe; ITU prowadziła do 1993 r. prace o charakterze normalizacyjnym w dwóch komitetach doradczych:

- **CCITT (International Consultative Committee on Telephony & Telegraphy)** - Komitet Konsultacyjny Telefonii i Telegrafii;
- **CCIR (International Consultative Committee on Radio)** - Międzynarodowy Doradczy Komitet Radiowy.

Oba komitety zostały rozwiązane, a na ich miejsce w marcu 1993 powstał ITU TSS (*ITU Telecommunication Standardization Sector*) - Dział Standardów Telekomunikacyjnych, który przejął nadzór nad całością zagadnień telekomunikacyjnych, w celu ujednolicenia i przyspieszenia prac w radio i telekomunikacji. Dokumentami opracowywanymi przez

ITU są zalecenia, powszechnie uznawane za nieformalne standardy światowe i przyjmowane za podstawę do opracowywania norm regionalnych i krajowych.

**izochroniczna transmisja** - sposób komunikacji zapewniający stałą szybkość transmisji, niezależnie od wielkości ruchu generowanego w otaczającym stację środowisku; polega na przydzieleniu kanału komunikacyjnego i egzekwowaniu stałego pasa przenoszenia. Kanał izochroniczny jest zwykle realizowany przez czasowe multipleksowanie pasa przenoszenia łączą telekomunikacyjnego i przydział stacji określonych (wymaganych) odcinków czasu. Transmisja izochroniczna jest niezbędna do obsługi ruchu multimedialnego.

**kable telekomunikacyjne** - szeroka klasa mediów stosowanych do transmisji sygnałów. Podstawowe znaczenie mają kable z przewodami miedzianymi i światłowodowe. Poza tą grupą znajdują się telekomunikacyjne media bezprzewodowe, obejmujące fale podczerwieni i mikrofale. Kable miedziane, powszechnie do tej pory stosowane mają szereg wad wynikających z ich właściwości elektrycznych. Należą do nich: ograniczająca zasięg rezystancja, emisja energii na zewnątrz kabla (umożliwiająca niepożądane monitorowanie transmitowanych przekazów) oraz podatność na wpływ promieniowania zewnętrznego, będącego przyczyną zniekształceń sygnału.

**kabel światłowodowy** - medium transmisyjne zbudowane z otoczonego nieprzeźroczystym płaszczem włókna kwarcowego o przekroju kołowym, w którym do przesyłania danych wykorzystuje się światło. Promienie świetlne (o częstotliwości w zakresie podczerwieni) ulegają w trakcie transmisji całkowitemu wewnętrznemu odbiciu, co powoduje, że promień prowadzony jest wzdłuż osi włókna. Światłowody charakteryzują się: dużą odpornością na zewnętrzne zakłócenia elektromagnetyczne, stopą błędów mniejszą niż  $10^{-10}$  przy najwyższych przepływnościach binarnych, małą tlumiennością jednostkową (zwykle ok. 0.20 dB/km) przy praktycznie zerowej dyspersji światłowodu. Światłowody umożliwiają budowę torów światłowodowych o przepływnościach do 10 Gb/s. Zasięg typowej linii światłowodowej (zbudowanej ze światłowodów jednomodowych), bez regeneracji sygnału za pomocą wzmacniaczy światłowodowych, wynosi od 80 do 100 km.

**klient/server** - model przetwarzania danych będący w istocie rozszerzeniem idei programowania modułarnego. W architekturze tej moduł wywołujący (zlecający usługę) staje się klientem, a moduł wywoływany (zapewniający usługę) - serwerem. Przetwarzanie w modelu klient-serwer zakłada możliwość jednoczesnej obsługi przez serwer żądań pochodzących od kilku klientów. Logiczną konsekwencją takiego rozszerzenia jest „posadzianie” klientów i serwerów na odpowiednich do ich funkcji platformach sprzętowych.

**kody transmisyjne** - sposoby konwersji ciągów sygnałów cyfrowych do innej, bardziej efektywnej postaci przy przesyłaniu przez szeregowe łączą cyfrowe, z uwzględnieniem fizycznych aspektów transmisji. Przy małych prędkościach transmisji (kb/s) konwersja zwykle nie jest realizowana. Oznacza to, że sygnały transmitowane w łączu fizycznym odpowiadają oryginalnym postaciom przesyłanych ciągów kodowych. Konwersja kodów cyfrowych do postaci i poziomów wymaganych przez konkretne medium transmisyjne (skrętka, koncentryk, światłowód) realizowana jest natomiast w przypadku dużych szybkości transmisji.

**kompresja (compression)** - technika pozwalająca ograniczyć nadmiarowość informacji i tym samym zmniejszyć objętość danych przed ich transmisją lub buforowaniem w pamięci. W modelu ISO-OSI kompresja dokonywana jest w warstwie prezentacji.

**komutacja** - sposób zestawiania połączeń (w tym kanałów rozmownych) w sieci telekomunikacyjnej. Wyróżnia się kilka technik komutacji. Najpopularniejsze to komutacja kanałów i komutacja pakietów, realizowana przez węzeł transmisyjny w trybie połącze-

niowym lub bezpołączeniowym. W przypadku komutacji kanałów, metody typowej dla systemów telefonicznych, przed rozpoczęciem przekazywania danych ma miejsce zestawianie połączenia fizycznego, a użytkownicy na czas połączenia uzyskują wyłączność na użytkowanie części przepustowości kanałów i zespołów połączeniowych. Cechą charakterystyczną komutacji pakietów jest z kolei możliwość czasowego przechowywania bloków danych w węzłach sieci. Komutacja pakietów z wykorzystaniem połączeń wirtualnych realizowana jest w sieciach ATM (komutacja komórek), a także sieciach X.25 i Frame Relay. Z kolei przykładem komutacji pakietów realizowanej w trybie bezpołączeniowym jest metoda komutacji datagramowej, stosowana w Internecie.

**LAN** - lokalna sieć komputerowa obejmująca swoim zasięgiem niewielki obszar (najczęściej budynek, przedsiębiorstwo). Standardy sieci lokalnych określają zasady organizacji pracy warstwy łączącej danych i warstwy fizycznej (IEEE 802.x). Do najpopularniejszych rozwiązań sieci LAN należą Ethernet, Token Ring, Token Bus. Najpopularniejszy, stale rozwijany standard - Ethernet (wykorzystujący algorytm dostępu do medium CSMA/CD) oferuje teoretyczną przepływność 10 Mb/s (generalnie od 1 Mb/s do 20 Mb/s). Jego szybsza wersja Fast Ethernet pozwala na realizację transmisji 100 Mb/s, zaś najnowsza Gigabit Ethernet gwarantuje przepływność 1Gb/s. Pozostałe standardy (Token Ring, Token Bus) oferują przepływności do 16 bądź 20 Mb/s. Równolegle z rozwojem protokołów sieci lokalnych, coraz większe znaczenie w sieciach LAN zdobywają też inne protokoły, wśród których dużą popularnością cieszy się oparty o technologię światłowodową protokół FDDI (będący w zasadzie typowym protokołem dla sieci metropolitannych) o przepływności 100 Mb/s a także standard ATM pozwalający na realizację transmisji z szybkościami od 25 Mb/s do 155 Mb/s (a nawet 622 Mb/s). Współpraca standardu ATM z sieciami lokalnymi jest możliwa dzięki np. standardowi LANE, emulacji sieci LAN w sieci ATM.

**LAN Emulation (LANE)** - standard ATM Forum umożliwiający integrację technologii ATM z tradycyjnymi technologiami sieci lokalnych Ethernet i Token Ring. Główną funkcją standardu LANE jest emulacja lokalnej sieci komputerowej w strukturze ATM. Definiuje on zasady dopasowania standardów sieci lokalnych, a także określa interfejs użytkowy dla protokołów warstw wyższych. Implementacja ATM w formie LANE nie wymaga żadnych modyfikacji protokołów warstw wyższych, ponieważ protokoły LANE prezentują te same interfejsy co protokoły MAC. W 1995 ATM Forum przyjęło standard LANE 1.0. W chwili obecnej opracowywana jest wersja 2.0, która definiuje rozproszoną architekturę LAN Emulation.

**LAN Emulation Client (LEC)** - w standardzie LANE obiekt końcowy systemu ATM, którego zakres zadań obejmuje między innymi: przesyłanie danych, analizę adresów oraz inne funkcje kontrolne realizowane w ramach pojedynczej sieci ELAN. LEC zapewnia standardowy interfejs użytkownika procesom warstw wyższych. LEC zawiera także interfejs LUNI (*LAN Emulation User Network Interface*) dla komunikacji z innymi elementami LANE. Każdy system końcowy, podłączony do sieci ELAN posiada jeden obiekt LEC na jeden ELAN. Z kolei każdy LEC jest identyfikowany poprzez unikatowy adres ATM i jest związany z jednym lub więcej adresami MAC osiągalnymi poprzez adres ATM. Ta druga sytuacja ma miejsce gdy klientem LEC staje się most lub przełącznik sieci LAN. Wówczas jeden LEC będzie związany z wszystkimi adresami MAC osiągalnymi poprzez porty tego przełącznika sieci LAN. Należy wziąć pod uwagę i to, że zbiór tych adresów MAC może ulegać dynamicznej zmianie. Obecne specyfikacje LANE definiują dwa typy sieci ELAN (802.3 i 802.5); nie dopuszczając jednak do bezpośredniego połączenia między klientami LEC, funkcjonującymi w ramach odmien-

nnych standardów LAN, np. LEC z segmentu Ethernet nie może bezpośrednio komunikować się z LEC z Token Ringu. Problem komunikacji pomiędzy tymi dwiema sieciami jest rozwiązywany na poziomie połączeń poprzez router ATM, który funkcjonuje jako klient w każdej z wymienionych sieci ELAN.

**LAN Emulation Configuration Server (LECS)** - serwer prowadzący, w standardzie LANE, ewidencję funkcjonujących sieci ELAN wraz z ich podstawowymi parametrami. Każdy obiekt, np. klient LEC, rozpoczynający pracę zgodnie z protokołem LANE, musi znać adres serwera LECS. W celu nawiązania połączenia z tym serwerem wysyła on podczas procesu inicjowania połączenia szereg zapytań skierowanych do LECS, chcąc uzyskać informacje między innymi o adresie serwera LES, o wielkości ramki oraz o typie medium. LECS przyporządkowuje klientów LEC do poszczególnych sieci ELAN oraz kieruje ich do odpowiednich serwerów LES. Obecne normy określają istnienie tylko jednego serwera LECS w całej domenie (sieci) ATM, obsługującego wszystkie sieci ELAN. Wersja 2 standardu LANE przewiduje możliwość instalowania kilku serwerów LECS. Informacje przechowywane w serwerze LECS są wprowadzane do niego przez administratora sieci.

**LAN Emulation Server (LES)** - obiekt implementujący, w standardzie LANE, funkcje kontroli w poszczególnych ELANach, posiadający unikatowy adres ATM. Przynależność do danej sieci ELAN oznacza związek z domenowym serwerem LES. LES prowadzi rejestrację adresów stacji sieci ELAN. W tym celu dokonuje analizy i rejestracji adresów MAC stacji a także wyznaczania tych adresów i ich odwzorowywania na adresy ATM (i/lub deskryptory tras do właściwych adresów ATM). W obrębie pojedynczej sieci ELAN może istnieć tylko jeden serwer LES. Górnny limit liczby stacji w sieci ELAN wyznaczany jest poprzez maksymalną liczbę identyfikatorów LEC, które mogą być zarejestrowane w serwerze LES (liczba ta wynosi 65279).

**iącze logiczne** - tymczasowe połączenie pomiędzy węzłami źródłowym i odbiorczym (docelowym), względnie pomiędzy procesami w obrębie jednego węzła, traktowane przez użytkowników końcowych jako iącze fizyczne.

**iącze satelitarne** - wydzielony czasowo (TDMA - *Time Division Multiple Access*) lub częstotliwościowo (FDMA - *Frequency Division Multiple Access*) kanał przekaźnika satelitarnego (transpondera). Pasmo przenoszenia satelity dzielone jest na dwa fragmenty: pasmo górne (*uplink*) - wykorzystywane do przesyłania z Ziemi do przekaźnika satelitarnego oraz pasmo dolne (*downlink*) - stosowane do transmisji z transpondera do stacji naziemnych.

**LIS (Logical IP Subnetwork)** - logiczna podsieć IP (w specyfikacji protokołu IPoATM) definiowana jako grupa stacji i routerów dołączonych do jednej sieci ATM i tworzących zamkniętą logiczną podsieć IP.

**LLC (Logical Link Control)** - górna podwarstwa warstwy iącza danych definiowana w architekturze sieci LAN w postaci standardu IEEE 802.2. Jej funkcje obejmują między innymi usługi świadczone przez LLC (bezołączniowe LLC-1, połączniowe LLC-2 oraz bezpołączniowe bez potwierdzeń LLC-3) a także zasady sterowania przesyłaniem ramek. Implementowany w LLC protokół sterowania przepływem ramek może być traktowany jako jedna z opcji protokołu HDLC.

**iącze transmisji danych** - zespół środków technicznych służących do transmisji szeregowej binarnych sygnałów danych wymienianych między dwiema stacjami sieci teleinformatycznej. Podstawowym medium transmisyjnym jest podkładowy kanał telefoniczny o standardowym pasmie zawartym między 300 a 3400 Hz. Cyfrowy charakter przesyła-

nej informacji wymaga zwykle przekształcenia sygnałów dyskretnych w analogowe za pomocą modemu po stronie nadawczej i przekształcenia odwrotnego po stronie odbiorczej. Łącze transmisji danych obejmuje kanał telefoniczny, urządzenia komutacji i podłączone z obu stron modem. Ze względu na tryb transmisji różnią się iącza: dwukierunkowe (*full duplex*), dwukierunkowe naprzemienne (*half duplex*) i jednokierunkowe (*simplex*).

**MAC (Medium Access Control)** - definiowana w sieciach lokalnych dolna część warstwy iącza danych modelu OSI. Podwarstwa MAC realizuje rozproszony algorytm dostępu do medium komunikacyjnego. Jest ona również odpowiedzialna za adresowanie w sieci LAN (adresy fizyczne MAC) oraz kontrolę błędów. Na podstawie pakietów otrzymywanych z warstw wyższych w podwarstwie MAC tworzone są ramki.

**mainframe** - szybki, wielodostępowy system komputerowy, zaprojektowany do przetwarzania dużej liczby danych i specjalizowanych zadań. Komputery o dużej mocy obliczeniowej - zwykle instalowane w większych firmach, uniwersytetach i organizacjach militarnych - mogą mieć setki, a nawet tysiące użytkowników. Ze względu na postępującą miniaturyzację podzespołów komputera właściwym kryterium określania mainframe nie jest jego wielkość, lecz moc obliczeniowa, zasoby pamięciowe i wielodostęp, a także wysoka jakość systemów operacyjnych i oprogramowania narzędziowego. Moc obliczeniowa średniej klasy komputera mainframe wynosi około 15000 MIPS (realizowanych przez komputer liczby operacji elementarnych na sekundę).

**MAN (Metropolitan Area Network)** - miejska (metropolitalna) sieć rdzeniowa określana też mianem sieci szkieletowej (*backbone*) o zasięgu rzędu 100 km; realizowana zwykle przy użyciu połączeń światłowodowych o wysokiej przepływności i niskiej stopie błędów; w węzłach światłowodowej sieci MAN ma miejsce konwersja sygnałów z postaci optycznej na elektryczną i odwrotnie; w sieciach MAN trzecie generacji konwersja sygnałów przebiega już wyłącznie w punktach końcowych fizycznego połączenia nadawcy z odbiorcą. Do tej pory opracowano dwa podstawowe standardy sieci metropolitalnych: FDDI (standard ANSI) i DQDB (standard IEEE), oba z zastosowaniem podwójnej magistrali światłowodowej przenoszącej sygnały optyczne jednocześnie w dwóch wzajemnie przeciwnych kierunkach. Podwójna magistrala ma najczęściej topologię pierścienia (w przypadku DQDB oznacza to generację wieloramek w magistralach przez jedną stację sieci), w którym w razie awarii kabla następuje automatyczna rekonfiguracja magistrali i kierunku obiegu danych. Uszkodzenie kabla w dwóch miejscach dzieli magistralę na dwie podsieci, działające niezależnie do czasu usunięcia awarii. Zasięg sieci MAN nie jest istotnym ograniczeniem: stosowanie jednomodowych włókien światłowodowych z thumieniem w trzecim oknie transmisyjnym wynoszącym średnio 0.20 dB/km daje swobodę w konfigurowaniu sieci, nawet na rozległym terenie. Postęp w technologii wzmacniaczy optycznych (o wzmacnieniu 20-30 dB dla pasma ok. 4000 GHz) umożliwia już tworzenie sieci MAN o gigabitowej przepływności optycznej i oferujących obsługę aplikacji czasu rzeczywistego (dane, głoś, dźwięk, obraz, wideo). Do tworzenia sieci MAN wykorzystywana jest przede wszystkim technika FDDI. Ostatnio coraz częściej wykorzystywane są też przełączniki ATM i zasady komutacji typowe dla sieci ATM.

**MIB** - lokalna baza danych w węźle sieci komputerowej, wykorzystywana do przechowywania informacji (atributów) o zarządzanym węźle i elementach sieci przyłączonych do węzła. Za aktualizację i modyfikację danych w MIB odpowiada program - agent znajdujący się w węźle sieci, współpracujący z programem - menedżerem SNMP stacji zarządzającej siecią. Specyficzne komendy i odpowiedzi według protokołu - SNMP, zainstalowanego w stacji zarządzania umożliwiają ocenę stanu węzła oraz informacji

przydatnych do wyciągnięcia wniosków na temat pracy całej sieci przez administratora systemu.

**model OSI** - opracowany przez ISO warstwowy model architektury, opisujący współdziałanie systemów otwartych. W modelu warstwowym pełny zbiór funkcji komunikacyjnych zostaje podzielony na podzbiory w taki sposób, by było możliwe traktowanie każdego jako pewnej całości wykonującej autonomiczne zadania. Wyodrębnione podzbiory funkcji są powiązane ze sobą tworząc strukturę hierarchiczną w postaci uporządkowanych warstw. Każda warstwa składa się z obiektów rozproszonych w różnych urządzeniach sieci komputerowej. Podstawową zasadą jest to, że komunikują się ze sobą tylko równorzędne pary obiektów jednej warstwy, korzystając jedynie z usług transmisji danych oferowanych przez warstwy niższe. Każda warstwa modelu jest opisana przez protokół (protokoły) wymiany informacji pomiędzy równorzędnymi obiektami warstwy oraz poprzez zbiór usług komunikacyjnych oferowanych warstwie znajdującej się bezpośrednio nad nią. Model odniesienia OSI składa się z siedmiu następujących warstw: fizycznej, łącza danych, sieciowej, transportowej, sesji, prezentacji, aplikacji.

**modem** - urządzenie stanowiące zakończenie sieciowe DCE, umożliwiające przyłączenie do publicznej, komutowanej sieci telefonicznej urządzenia o charakterze cyfrowym (komputer). Modem dokonuje konwersji sygnału cyfrowego na postać analogową, przesyłaną dalej przez łączę telekomunikacyjne. Inny modem, po drugiej stronie łącza realizuje operację odwrotną dokonując konwersji sygnału analogowego na cyfrowy.

**most** - proste urządzenie sieciowe wyposażone w co najmniej dwa porty wejścia/wyjścia. Każdy port dołączany jest do oddzielnego segmentu sieci LAN, umożliwiając ich wzajemną współpracę. Mosty operują w podwarstwie MAC warstwy łącza danych, pozwalając na stosowanie różnych standardów warstwy fizycznej modelu OSI. Istnieją dwa podstawowe typy mostów: mosty transparentne i źródłowe, różniące się metodą doboru tras w sieci.

**multipleksacja** - technika zwielokrotnienia i transmisji wielu sygnałów analogowych lub cyfrowych o niższej przepływności pojedynczym kanałem komunikacyjnym o dużej przepływności binarnej. Po drugiej stronie łącza zachodzi proces odwrotny, zwany demultipleskacją, odtwarzający pierwotne ciągi sygnałów.

**multiplekser statystyczny** - urządzenie, które poprzez analizę intensywności ruchu natrywającego z wielu źródeł wejściowych i czasowe buforowanie ruchu nadmiarowego zapobiega utracie części danych; zastosowane algorytmy statystyczne przydziela zasóbów (kanałów, ścieżek) pozwalają na dynamiczny przydział szczelin do przeciążonych kanałów; multipleksacja statystyczna stosowana jest np. w przełącznikach ATM.

**narzędzia i techniki diagnozowania sieci** - narzędzia diagnozowania sieci oparte są na dwóch podstawowych technikach: periodycznym rejestraniu określonych parametrów pracy urządzeń sieciowych oraz zgłaszaniu określonych zdarzeń. Okresowe rejestrowanie parametrów ma na celu przewidywanie wystąpienia sytuacji awaryjnych, natomiast zgłoszenie zdarzeń informuje o powstaniu awarii (odpowiednie dane oraz komunikaty są wysyłane przez agentów zainstalowanych na węzłach sieciowych i są rejestrowane przez stację zarządzającą). Innym sposobem diagnozowania sieci jest stosowanie analizatorów protokołów, dzięki którym możemy rejestrować i analizować przesyłane w sieci pakiety.

**NetBios** (*Network Basic input output system*) - protokół zaprojektowany przez firmę Microsoft i IBM w celu zapewnienia komunikacji w małych i średnich sieciach LAN; NetBios jest w istocie interfejsem API stosowanym do pisania aplikacji dla sieci lokalnych; nadaje on węzłom niepowtarzalne nazwy (do 15 znaków) i ustania sesje połączeniowe;

protokół połączeniowy tworzy między nadawcą a odbiorcą kanał logiczny, gwarantując dostarczenie wiadomości do adresata; NetBios oferuje połączenie datagramowe z innymi systemami; jest implementowany w sieciowych systemach operacyjnych IBM LAN Server, Microsoft LAN Manager i OS/2.

**NetWare** - sieciowy system operacyjny firmy Novell; oferowane są dwie zasadnicze odmiany różniące się koncepcją usług katalogowych: NetWare 3.x (Bindery) i NetWare 4.x (NDS); systemy NetWare działają w oparciu o model klient-serwer.

**NOS (Network Operating System)** - sieciowy system operacyjny pracujący na komputerach wchodzących w skład lokalnych sieci komputerowych; zarządzający pracą zarówno zasobów lokalnych, jak też przyłączonych za pośrednictwem sieci (LAN i WAN); dokonuje filtracji komend kierowanych bezpośrednio do systemu lokalnego bądź do serwera sieciowego; obsługuje protokoły komunikacyjne i zapewnia realizację podstawowych usług sieciowych (usługi katalogowe, współdzielenie plików, usługi adresowe itp.); do najpopularniejszych systemów można zaliczyć: NetWare firmy Novell, Windows NT firmy Microsoft, Vines firmy Banyan i LANtastic firmy Artisoft.

**NPC (Network Parameter Control)** - funkcja sterowania parametrami sieci ATM, kontrolująca intensywność strumienia komórek na styku sieć-sieć.

**NRM (Network Resource Management)** - funkcja zarządzania zasobami sieci ATM, odpowiadająca za podział zasobów sieciowych pomiędzy poszczególne odizolowane logicznie połączenia z uwzględnieniem rodzajów usług; wykorzystuje ona koncepcję ścieżek i kanałów wirtualnych.

**NRZ (Non Return to Zero)** (bez powrotu do zera) - jeden z popularnych kodów transmisyjnych, używający dwóch poziomów napięcia dla prezentacji wartości binarnych ciągu informacji; stosowany np. w sieciach FDDI (NRZ Inverted) łącznie z kodem 4B/5B gwarantującym brak występowania kolejno więcej niż trzech zer.

**NT (Windows NT)** - 32-bitowy system operacyjny firmy Microsoft, aktualnie dostępny w dwóch odmianach: Windows NT Serwer, który może pełnić rolę serwera sieciowego w sieciach komputerowych typu klient-serwer, oraz Windows NT Workstation dla stacji roboczych; systemy te charakteryzuje się rozbudowanym interfejsem graficznym użytkownika, wielozadaniowością z wywłaszczeniem (*pre-emptive multitasking*), ochroną pamięci i wieloprocesorością symetryczną; umożliwia użytkownikom współdzielenie plików z innymi użytkownikami oraz dostęp do współdzielonych katalogów w systemach innych użytkowników.

**ochrona danych** - mechanizmy ochrony danych mają na celu zabezpieczenie danych przed nieupoważnionym dostępem (zarówno odczytem jak i modyfikacją). Ochrona danych obejmuje różnorodne techniczne i nietechniczne środki zapobiegania nieautoryzowanemu dostępowi do danych, w tym utajniania przechowywanych i przesyłanych danych, zasady autoryzacji dostępu do zgromadzonych danych itp.

**okablowanie strukturalne** - całociwowy, wielofunkcyjny system okablowania wewnętrz budynku lub kampusu, przeznaczony do transmisji głosu (telefonia) i danych (sieć komputerowa), definiuje też zasady komunikacji zewnętrznej, w tym z łączami publicznej sieci telefonicznej, a także siecią pakietową; koncepcja okablowania strukturalnego uwzględnia niezbędną infrastrukturę telekomunikacyjną dla tych potrzeb składającą się z: (1) okablowania poziomego, łączącego naścieenne przyłącza użytkownika z dystrybutorami kondygnacyjnymi; (2) okablowania pionowego, łączącego kondygnacje budynków, bądź też budynki w kampusie między sobą lub z węzłem dystrybucyjnym budynku;

(3) międzybudynkowej magistrali szkieletowej, przeznaczonej również do połączeń z sieciami MAN. Topologia fizyczna sieci z okablowaniem strukturalnym jest zwykle gwiazdzista; możliwe jest jednak tworzenie innych topologii sieciowych - bez konieczności instalacji dodatkowych kabli.

**organizacje standaryzacyjne** (normalizacyjne) - można je sklasyfikować ze względu na terytorialny zakres działania (światowy/regionalny) oraz merytoryczny zakres działania (normalizacja branżowa/ogólna). Do najważniejszych organizacji standaryzacyjnych, które opracowują normy i standardy technologii teleinformatycznej zaliczyć można: ITU TSS (*ITU Telecommunication Standardization Sector*); ISO (organizacja, której członkowie zwyczajni to krajowe organizacje normalizacyjne oraz członkowie korespondenci to organizacje typu ECMA i IEEE); IEC - branżowy (elektryka i elektronika) komitet wydzielony z ISO, koordynuje prace wielu organizacji standaryzacyjnych; ETSI - instytut powołany przez EWG, zajmuje się normalizacją europejskiego rynku telekomunikacyjnego (sprzęt, sieci, usługi telekomunikacyjne); ANSI - reprezentant USA w ISO, skupia około 300 branżowych komitetów normalizacyjnych; IEEE - amerykańskie stowarzyszenie zawodowe; opracowało kilka istotnych standardów sieciowych (IEEE 802.x); IETF - komitet opracowujący propozycje standardów dla sieci Internet.

**PAD (Packet Assembler-Disassembler)** - urządzenie typu multipleksera stosowane w publicznych sieciach pakietowych X.25. Umożliwia, po stronie nadawczej, zamianę strumienia znaków ASCII, generowanego przez użytkownika, w pakiet danych zgodny z protokołem X.25, po stronie odbiorczej przekształca pakiety X.25 w pierwotny strumień znaków.

**pakiet** - strumień bitów składający się z danych oraz informacji sterujących zawierających między innymi adresy węzłów źródłowego oraz przeznaczenia, a także stosowne ciągi kontrolne zabezpieczające blok danych przed błędami.

**PC (Priority Control)** - funkcja (w sieci ATM) kontroli priorytetu, która w warunkach przeciążenia w sieci, decyduje o usunięciu z sieci komórek oznakowanych bitem CLP (*Cell Loss Priority*), tj. komórek o niższym priorytecie. Mechanizm kontroli bitu CLP może być także wykorzystywany przez funkcję UPC.

**peer to peer** - typ komunikacji warstwowej realizowanej między obiektami tej samej warstwy sieci komputerowej, zgodnie z którym wszystkie stacje robocze mają podobny stopień kontroli nad siecią; jest to metoda całkowicie odmienna od pierwszych systemów przetwarzania z komputerem mainframe, w których centralny komputer udostępniał całą moc przetwarzania, a terminale sieciowe ograniczały się do wprowadzania danych i prezentacji wyników. Obecnie prawie wszystkie sieciowe systemy operacyjne umożliwiają tworzenie sieci „równorzędnych”.

**plataforma zarządzania siecią** - wyspecjalizowane narzędzia programowe do monitorowania i zarządzania rozległą lub metropolitalną siecią komputerową; wykorzystuje jeden z dedykowanych protokołów (SNMP, CMIP, DMI, OSI) celem ustalenia liczby urządzeń, ich konfiguracji przestrzennej i logicznej; określa stan urządzeń, rekonfiguracji sieci i obciążenia segmentów sieci, potrzebę przetestowania urządzeń itp.; platformy można podzielić na dwie kategorie: oparte na systemie Unix oraz oparte na systemie Windows. Wybór odpowiedniej platformy jest związyany z oprogramowaniem systemowym, infrastrukturą sieci, liczbą urządzeń i sposobem obsługi stanów awaryjnych. Platformy oparte na Unixie są bardziej elastyczne i lepiej skalowalne od tańszych działających w środowisku Windows.

**poczta elektroniczna (e-mail)** - usługa sieciowa umożliwiająca przekazywanie komunikatów tekstowych i plików binarnych z zastosowaniem indywidualnych skrytek pocztó-

wych, pomiędzy komputerami połączonymi w sieć (LAN lub WAN) i ich użytkownikami. Istnieje wiele różnych implementacji poczty elektronicznej np. Novell GroupWise (wykorzystywany w sieciach LAN opartych o sieciowy system operacyjny Novell NetWare) czy też protokoły SMTP/POP3 wykorzystywane w sieci Internet.

**podsieć** - wydzielona fizycznie i/lub logicznie sieć komputerowa, która ze względów administracyjnych, przeznaczenia, potrzeb użytkowników odróżnia się od pozostałe części sieci.

**połączenia wielopunktowe** - połączenia, w których liczba odbiorców przesyłanych danych jest większa niż jeden (stosowane np. w usługach multimedialnych - wideokonferencje).

**połączenie wirtualne (virtual circuit)** - trasa poprzez sieć, która może być postrzegana przez użytkowników końcowych (procesy) w połączeniu typu end-to-end jako połączenie fizyczne. W rzeczywistości jest to dynamicznie modyfikowane połączenie sieciowe, uaktyniane w określonych przedziałach czasu.

**PPP (Point to Point Protocol)** - standardowy protokół typu punkt-punkt warstwy sieciowej Internetu, gwarantujący niezawodną transmisję w komutowanych lub stałych łączach szeregowych bez ograniczania szybkości; jeden z dwóch datagramowych protokołów IP (PPP, SLIP). PPP może obsługiwać zarówno bitowo zorientowaną transmisję synchroniczną, jak też zorientowaną bajtowo asynchroniczną transmisję danych.

**procesor komunikacyjny** - komputer pośredniczący w komunikacji pomiędzy komputerem głównym (hostem) i siecią urządzeń końcowych. Głównym zadaniem procesora komunikacyjnego jest odciążenie hosta od zadań związanych z obsługą urządzeń zewnętrznych.

**protokół komunikacyjny** - zestaw procedur zapewniających komunikację między komputerami, systemami końcowymi i węzłami sieci. Obejmuje on reguły wyboru trasy, procedury tworzenia pakietów/ramek jak też algorytm dostępu do medium; różne protokoły komunikacyjne mogą znacznie różnić się między sobą zaimplementowanymi funkcjami.

**przelaczanie (switching)** - metoda zestawiania połączeń w rozproszonych sieciach cyfrowych o heterogenicznym charakterze. Umożliwia realizację głównie usług bezpołączeniowych (przekaz datagramów), jak też usług połączeniowych wymagających przed przekazaniem informacji zestawienia łącz. Logiczna konfiguracja sieci (topologia), składająca się z fizycznych segmentów sieci, obejmuje kanały wirtualne, oparte na istniejących, fizycznych kanałach transmisji. Kanały wirtualne są komutowane przez przełączniki i węzły sieci, tworząc połączenia alternatywne, w przypadku uszkodzenia, przeciążenia lub zablokowania podstawowych kierunków transmisji danych.

**przełącznik ATM** - zasadnicza część węzła sieci ATM zapewniająca bezkolizyjne i dynamiczne multipleksowanie ścieżek i kanałów wirtualnych w jeden strumień lub kilka strumieni cyfrowych, łączących poszczególne węzły sieci.

**przełącznik LAN** - urządzenie umożliwiające łączenie wielu komputerów w sieć o topologii gwiazdzistej, wyposażone w pewną liczbę portów dla stacji roboczych pracujących w standardzie Ethernet (*Fast Ethernet*). Przełączniki zastępują popularne dotychczas huby. Przełącznik LAN rozróżnia dołączone do swoich portów adaptery sieciowe poszczególnych stacji na podstawie ich adresów sieciowych MAC. Każda otrzymana ramka jest analizowana i propagowana tylko na jednym porcie, do którego podłączony jest adapter o adresie MAC zgodnym z adresem MAC przeznaczenia ramki. W znaczący sposób obniża to ruch w sieci.

**przetwarzanie rozproszone** - sposób przetwarzania danych, zgodnie z którym obliczenia użytkownika (jeden program) są wykonywane równocześnie na kilku komputerach sieci (każdy komputer dokonuje własnych obliczeń na przydzielonych mu danych), a sieć zapewnia wymianę danych oraz synchronizację przetwarzania.

**przetwarzanie równolegle** - przetwarzanie analogiczne do przetwarzania rozproszonego z tą różnicą, że rolę stacji przejmują procesory, a sieć zastępowana jest wewnętrzna magistralą komputera (nieformalnie przetwarzanie równolegle związane jest z przetwarzaniem na maszynach wieloprocesorowych, podczas gdy przetwarzanie rozproszone to przetwarzanie w sieci). Ponadto przetwarzanie równolegle różni się od przetwarzania rozproszonego krótszym czasem komunikacji. W przypadku przetwarzania rozproszonego węzły dokonujące obliczeń posiadają najczęściej własną pamięć; w systemach równoległych pamięć jest zwykle dzielona przez jednostki obliczeniowe (procesory).

**przejrzystość (transparency)** - cecha systemu lub tryb transmisji, zgodnie z którym jednostki danych są przesyłane przez system bez jakiegokolwiek ich modyfikacji.

**PSDN (Public Switched Data Network)** - publiczna sieć transmisji danych działająca w trybie pakietowym.

**PSTN (Public Switched Telephone Network)** - infrastruktura telekomunikacyjna o charakterze publicznym, oparta na komutacji łącz (linii telefonicznych); pierwotnie, usługi sieci PSTN dotyczyły głównie automatycznej komutacji kanałów rozmównych; lista świadczonych usług jest stopniowo powiększana o usługi rozszerzone i dodatkowe związane z wprowadzeniem bardziej inteligentnych systemów komutacji.

**QoS (Quality of Service parameters)** - jakość obsługi definiowana dla sieci ATM przez zbiór parametrów, wśród których najważniejsze to: maksymalne opóźnienie przesłania komórki przez sieć MaxCTD (Maximum Cell Transfer Delay), zmienność opóźnienia w przekazie komórek - CDV (Peak-to-peak Cell Delay Variation) oraz prawdopodobieństwo CLR straty komórki (Cell Loss Ratio).

**radiokomunikacja ruchoma** - szeroko pojęta komunikacja bezprzewodowa, rozwijana z przeznaczeniem dla abonentów znajdujących się w ruchu. Wstępnie uzgodnione i będące na etapie standaryzacji nowe generacje systemów komunikacji ruchomej umożliwiają szeroki zakres usług multimedialnych. Bezprzewodowa komunikacja z szybkością 2Mb/s, dostępna za pomocą podręcznego kieszonkowego radiotelefonu, zapewni przesyłanie głosu, danych, faksu i obrazów oraz ciągłą lokalizację i identyfikację abonenta w dowolnym miejscu. Do najbardziej zaawansowanych projektów komunikacji ruchomej, przewidzianych do realizacji do roku 2005, należą systemy uniwersalnej łączności ruchomej UMTS, FPLMTS oraz MBS.

**ramka komunikacyjna** - określona struktura danych cyfrowych przesyłanych strumieniem szeregowym przez kanał komunikacyjny. Wyróżnia się dwa podstawowe typy ramek: informacyjne i organizacyjne. W ramkach definiowane są zwykle pola nagłówka służące do sterowania ruchem i kontroli poprawności transmisji oraz pole danych.

**regenerator sygnału (repeater)** - aktywny element sieci służący do wzmacniania sygnału w celu zwiększenia zasięgu transmisji poza dopuszczalną długość kabla. Zdefiniowany w warstwie fizycznej modelu OSI nie modyfikuje sygnałów, przywracając jedynie zniekształconym impulsom ich pierwotną formę.

**RMON (Remote MONitoring)** - jedna z dwóch metod zdalnego monitorowania sieci komputerowej z zastosowaniem tzw. sondy RMON. Drugim sposobem przeprowadzenia analizy pracy sieci lokalnych są analizatory protokołów sieciowych. Sondy RMON deko-

dują protokoły (warstwa po warstwie) i badają wskazany strumień danych. W odróżnieniu od analizatorów sondy są zaprojektowane pod kątem stałego ich umiejscowienia w kilku węzłach sieci o szczególnej aktywności, a połączone z jednym urządzeniem sterującym - wyposażonym w interfejs graficzny - umożliwiają tworzenie kompleksowych zestawów informacji dla optymalnego prowadzenia sieci.

**router** - urządzenie sieciowe wyposażone w co najmniej dwa porty wejścia/wyjścia, umożliwiające integrację segmentów sieci LAN, sieci LAN z sieciami WAN, bądź sieci WAN. Router operuje w warstwie sieciowej modelu OSI, pozwalając na stosowanie różnych standardów warstwy fizycznej oraz warstwy łączącej danych. Do każdego portu może być podłączonych wiele adapterów sieciowych (tworzących sieć komputerową), należących do tej samej klasy adresowej. Router analizuje każdą ramkę i przesyła ją na odpowiedni port zgodnie z jej adresem przeznaczenia (adresem warstwy sieciowej), według wewnętrznej tablicy routingu.

**routing** - mechanizm doboru tras pakietów w sieciach WAN i MAN. Routing w Internecie, oparty jest o mechanizm adresowania realizowany przez protokół warstwy sieciowej IP. Wyróżnia się dwie podstawowe klasy routingu: routing statyczny, w którym wszystkie trasy pakietów w sieci są ustalone na sztywno oraz routing dynamiczny, w którym trasy pakietów są dobierane dynamicznie, uwzględniając aktualną topologię i obciążenie sieci. W sieciach WAN wykorzystanie znajduje tzw. routing hierarchiczny. Zgodnie z nim wyróżnia się routing wewnętrzny (lokalny danej domeny) i zewnętrzny. Routing wewnętrzny w Internecie wykorzystuje protokoły RIP i OSPF.

**RS (Recommended Standard)** - zbiór standardów określonych przez EIA (Electronic Industries Association), opisujących sposób podłączenia urządzenia o charakterze cyfrowym (komputer - DTE) do urządzenia periferyjnego sieci zorientowanego znakowo (DCE). Najbardziej popularnym standardem serii RS jest standard RS232C.

**SDLC (Synchronous Data Link Protocol)** - zorientowany bitowo protokół warstwy łączącej danych opracowany przez firmę IBM. Jest on pierwowzorem popularnego protokołu warstwy łączącej danych HDLC.

**segment sieci** - wydzielony fizycznie fragment sieci lokalnej (odpowiednik magistrali sieci Ethernet oraz domeny kolizyjnej). Segmente mogą być łączone ze sobą lub z siecią rozległą za pomocą węzłów sprzągających (most, przełącznik LAN, router). Segmentacja dużej sieci zwiększa jej przepływność (pakiet w jednym segmencie nie koliduje z ruchem w pozostałych segmentach). Przełączniki LAN umożliwiają wprowadzenie mikrosegmentacji (jedna stacja na segment).

**serwer** - węzeł sieci (komputer) udostępniający pozostały węzłom sieci (komputerom) usługi sieciowe różnego rodzaju. W zależności od typu sieci istnieje wiele rodzajów usług udostępnianych przez serwer. Dla sieci lokalnych podstawowe usługi oferowane przez serwer to współdzielenie zasobów takich jak systemy plików czy systemy druku, dla sieci rozległych do podstawowych oferowanych usług należą usługi pocztowe, WWW, NFS czy też FTP.

**sieć bezprzewodowa** - sieć telekomunikacyjna (również komputerowa) wykorzystująca systemy transmisji radiowej lub systemy łączności na podczerwieni jako medium transmisyjne. W sieciach bezprzewodowych LAN podstawowymi standardami są: IEEE 802.11 i ETSI HIPELAN.

**sieć szkieletowa (backbone)** - w sieciach LAN i MAN jest to segment sieci (pętla lub magistrala) wykorzystany do obsługi dużego ruchu. Sieć szkieletowa nazywana też rdzeniowa

łączy zwykłe segmenty sieci komputerowej wewnątrz budynków; stanowi także podstawowy środek transportu w sieciach MAN - nazywany często magistralą osiową. Ze względu na sposób przyłączenia segmentów sieci LAN do sieci szkieletowej wyróżnia się: (1) złożone sieci szkieletowe (*backbone network*), w których segmenty sieci LAN są dołączane za pośrednictwem mostów i routerów; (2) proste sieci szkieletowe (*collapsed backbone*), z pojedynczym hubem łączącym gwiazdzieście segmenty lokalne.

**SMTP (Simple Mail Transfer Protocol)** - jedna z podstawowych aplikacji w stanie TCP/IP realizująca popularną usługę poczty elektronicznej (*email*). Protokół SMTP umożliwia przesyłanie dowolnych wiadomości reprezentowanych jako ciąg znaków ASCII pomiędzy elektronicznymi systemami pocztowymi. Protokół definiuje sposób transmisji; struktura transmitowanych danych jest podana w zaleceniu RFC 822.

**SNA (System Network Architecture)** - warstwowa architektura sieciowa opracowana dla potrzeb sieci IBM. Podobnie jak w modelu ISO-OSI definiowane są warstwy realizujące ściśle określone funkcje. Odmiennie niż w modelu ISO-OSI przebiegają procesy zestawiania połączenia. Zamiast komunikacji typu peer-to-peer mamy tutaj ściśle skoncentrowane mechanizmy sterowania połączeniem i wyraźnie zarysowaną hierarchię sprzętową.

**SNMP (Simple Network Management Protocol)** - protokół warstwy aplikacji umożliwiający zarządzanie protokołami komunikacyjnymi sieci TCP/IP. Wykorzystuje koncepcję menedżer-agent. Aplikacja menedżera rezyduje w module zarządzającym, zbierając informacje o stanie urządzeń za pośrednictwem rezydujących w tych urządzeniach tzw. agentów SNMP. Umożliwia zarządzanie różnorodnymi elementami sieci komputerowej np. bezpieczeństwem, wydajnością.

**stacja robocza** - węzeł sieci (komputer) wykorzystujący podczas pracy usługi oferowane przez serwery sieciowe.

**STP (Shielded Twisted Pair)** - skrętka ekranowana - para skręconych, izolowanych przewodów umieszczonych we wspólnie osłoniętej izolacyjnej dodatkowo chronionej przez specjalny ekran. Charakterystyczną wartością skrętki jest jej przekrój poprzeczny wyrażany w jednostkach AWG. Podstawowe cechy skrętki ekranowanej: symetryczność, mały ciężar, szerokie pasmo przenoszenia, mała tlumienność oraz mała wrażliwość na zakłócenia zewnętrzne (ze względu na ekran).

**styk (interface)** - standardowy układ lub oprogramowanie, pełniące rolę elementu pośredniczącego przy współpracy systemów lub urządzeń. Najpopularniejsze styki fizyczne np. typu RS specyfikowane przez EIA i służące do transmisji szeregowej definiują wymiary gniazd i wtyków, sygnały elektryczne i ich wartości, procedury związane z przekazywaniem sygnałów. Styk programowy definiuje zasady współpracy np. między-warstwowej, w tym procedury realizacji komunikacji między odmiennymi obiektami.

**styk użytkownik-sieć-UNI (User-Network Interface)** - określa zasady połączenia stacji komputerowej użytkownika z siecią ATM. Istnieją dwa rodzaje interfejsów UNI: prywatny UNI (odnosi się do styku pomiędzy użytkownikiem, a systemem komutacyjnym - przełącznikiem ATM należącym do tej samej sieci co użytkownik i publiczny UNI (wykorzystywany przy łączeniu użytkownika z publiczną siecią ATM; z interfejsem tym związany jest protokół ILMI (*Interim Local Management Interface*)).

**styk sieć-sieć-NNI (Network-Network Interface lub Network-Node Interface)** - opisuje zasady łączenia przełączników ATM i odpowiada za zarządzanie ich współdziałaniem. Istnieją dwa rodzaje styków NNI: prywatny - dotyczący przełączników w prywatnych sieciach oraz NNI publiczny, stosowany w sieciach publicznych.

**synchroniczna transmisja** - tryb transmisji, w którym dane przesyłane są łączem w sposób ciągły (bez znaków startu i stopu jak dla transmisji asynchronicznej). Zegary nadajnika i odbiornika pozostają w ciągłej synchronizacji. W związku z tym stosowane są odpowiednie metody synchronizacji bitowej, znakowej oraz ramki. Istnieją dwa typy transmisji synchronicznej: zorientowany znakowo (starsze protokoły np. BSC i DDCMP) oraz bitowy (obecnie najczęściej stosowane są różne wersje HDLC). Oba typy transmisji wykorzystują te same metody synchronizacji bitowej, inne dla synchronizacji znakowej i ramki.

**systemy otwarte** - systemy komputerowe oraz komunikacyjne pochodzące od różnych producentów, ale oparte na powszechnie znanych i dostępnych standardach. Dostęp do specyfikacji technicznych umożliwia wprowadzanie modyfikacji i rozbudowy systemów otwartych przez użytkowników tych systemów.

**systemy wieloprocesorowe** - systemy posiadające więcej niż jeden procesor (jednostkę centralną). Wszystkie procesory współdzielą szynę komputera, a niekiedy również pamięć i urządzenia zewnętrzne. Głównym powodem konstruowania systemów wieloprocesorowych jest dążenie do zwiększenia mocy obliczeniowej (podział zadań) oraz niezawodności (nadmiarowe jednostki centralne). W przeważającej większości używanych obecnie systemów wieloprocesorowych stosuje się model wieloprzetwarzania symetrycznego, w którym na każdym procesorze działa identyczna kopia systemu operacyjnego (kopie te komunikują się ze sobą w zależności od potrzeb). W niektórych systemach stosuje się wieloprzetwarzanie asymetryczne polegające na przydzieleniu każdemu procesorowi specyficznego zadania.

**szeregowa transmisja** - transmisja, w której dane są nadawane i odbierane z wykorzystaniem pojedynczych przewodów oznaczanych jako TX, RX. Kontrola transmisji odbywa się poprzez wykorzystanie linii kontrolnych pomiędzy DTE i DCE (np. RTS/CTS). Możliwa jest praca w trybie synchronicznym i asynchronicznym.

**szerokość pasma** - wyrażony w hertzach (Hz) zakres częstotliwości (różnica pomiędzy górną a dolną częstotliwością pasma), który jest zdolny przenieść kanał telekomunikacyjny, bądź też część pasma transmisyjnego udostępniana dla określonych usług sieciowych czy też komunikujących się użytkowników. Przykładowo szerokość pasma dla kanału telefonicznego wynosi 3,1 kHz (w paśmie naturalnym od 300 Hz do 3400 Hz). Zdolność kanału do przenoszenia informacji binarnej (przepływność wyrażana w b/s) jest proporcjonalna do szerokości pasma transmisji.

**szynkość modulacji (baud rate)** - jest to szybkość z jaką wybrany parametr (faza, amplituda, częstotliwość) sygnału nośnego ulega zmianie. Oznacza liczbę sygnałów elementarnych, które można przesłać w ciągu jednej sekundy. Szybkość modulacji w powiązaniu ze stosowanym kodowaniem pozwala określić szybkość bitową transmisji.

**szynkość transmisji** - inaczej zwana prędkością bitową lub przepływnością oznacza liczbę bitów, które mogą być przesłane z wykorzystaniem danego łączna transmisyjnego w jednostce czasu (najczęściej na sekundę). Szybkość transmisji z wykorzystaniem łączni sieci telefonicznej jest zależna od szybkości modulacji, jej typu oraz sposobu kodowania strumienia danych.

**światłowód** - medium transmisyjne zbudowane z otoczonego nieprzezroczystym płaszczem szklanego włókna kwarcowego o przekroju kołowym, w którym do przesyłania danych wykorzystuje się światło. Promienie światłowe (o częstotliwości w zakresie podczerwieni) ulegają w trakcie transmisji całkowitemu wewnętrznemu odbiciu, co powoduje, że promień jest prowadzony wzduż osi włókna. Włókna światłowodowe klasyfikuje

się według ich średnicy, tlumienności, dyspersji, zakresu zmian współczynnika załamania oraz liczby prowadzonych modów (promieni wiązki świetlnej).

**TCP/IP** - termin określający zbiór popularnych protokołów komunikacyjnych stosowanych w sieci rozległej Internet, obejmujący między innymi protokoły IP, TCP, UDP oraz protokoły warstw wyższych wykorzystywane w sieci Internet. Dla opisu protokołów stoso TCP/IP stosuje się uproszczony, czterowarstwowy model odniesienia. Protokół IP jest protokołem warstwy sieciowej oferującym usługi bezpołączeniowe. Protokół TCP jest połączniowym protokołem warstwy transportowej. Protokół UDP jest bezpołączeniowym protokołem warstwy transportowej. Pozostałe protokoły definiują różne usługi sieciowe warstw wyższych np. SMTP - usługi pocztowe, HTTP - usługi WWW.

**token** - specjalny typ ramki kontrolno-organizacyjnej, przesyłanej między stacjami sieci, zapewniający bezkolizyjny i zazwyczaj cykliczny dostęp do medium. Tylko stacja przesyłająca token (znacznik) ma prawo do przesłania danych. Algorytmy tokenowe (token passing) są popularnymi rozwiązaniami stosowanymi w sieciach LAN (IEEE 802.4 i 802.5).

**Token Bus** - standardowe rozwiązanie sieci LAN (standard IEEE 802.4) o topologii magistrali (ogólnie drzewa) i deterministyczno-tokenowej zasadzie dostępu. Procedura dostępu zbliżona do implementowanej w sieci Token Ring, polega na wymianie między aktywnymi stacjami sieci, powiązanymi w tzw. pętlę logiczną, specjalnej, adresowej ramki sterującej określonej mianem tokena (znacznika). Tylko stacja będąca adresatem tokena nabywa prawa dostępu do medium i transmisji ramek informacyjnych. Dostęp do sieci uzyskiwany jest przy tym cyklicznie z wykorzystaniem procedur wyznaczających nominalny i rzeczywisty czas obiegu tokena wokół pętli logicznej (*target token rotation time* i *token rotation time*). Standard pozwala na nadawanie przesyłanym ramkom priorytetów. Najwyższy priorytet (określany jako priorytet poziomu 6) mają tzw. ramki synchroniczne, których obsługa związana jest z ostrymi ograniczeniami czasowymi. Protokół Token Bus ma bardzo rozbudowane procedury utrzymywane, w szczególności określające działania podejmowane przez stacje w sytuacjach awaryjnych. Standard definiuje szereg szybkości transmisji 1, 5, 10 i 20 Mb/s, realizowanych w trybie baseband, carrier-band lub broadband z wykorzystaniem głównie kabli koncentrycznych i światłowodów.

**Token Ring** - standardowe rozwiązanie LAN (IEEE 802.5) wspierane przez IBM. Sieć Token Ring wykorzystuje topografię pierścieniową. Transmisja danych przez stację odbywa się po przechwytceniu przez stację specjalnego znacznika (*Tokena*), będącego ramką kontrolną protokołu. Możliwe jest stosowanie kilku poziomów priorytetów, co pozwala na obsługę ruchu synchronicznego. Najpopularniejsze implementacje protokołu Token Ring oferują przepływności rzędu 16 Mb/s (inne szybkości specyfikowane przez standard to 1 i 4 Mb/s).

**topologia sieci** - sposób fizycznego połączenia węzłów (komputerów) w sieć komputerową, zapewniający możliwość przesyłania danych do wszystkich stacji. Do podstawowych topologii wykorzystywanych w sieciach LAN należą konfiguracje: magistralowa, drzewiasta, pierścieniowa, gwiazdista oraz topologia rozproszona (*mash*) charakterystyczna dla sieci WAN.

**TS (Traffic Shaping)** - funkcja kształtuowania ruchu w sieci ATM pozwalająca wpływać na charakterystykę ruchu generowanego przez użytkownika, w celu dopasowania tej charakterystyki do deklaracji złożonej w fazie zestawiania połączenia.

**UBR (Unspecified Bit Rate)** - usługa o niezdefiniowanej szybkości bitowej - przewidziana dla źródeł o niezdefiniowanej szybkości transmisji, realizujących niregularny przekaz danych, w miarę dostępności łączka. W przypadku stosowania usługi UBR, aplikacja wysyła

dane w sieć i nie interesuje się, czy i kiedy dane te dotrą do celu. Sieć z kolei postępuje zgodnie z zasadą największego wysiłku tj. „*best effort*”. W związku z tym, w momentach przeciążenia łącza usługami innych typów dane przesyłane w ramach UBR są po prostu tracone.

**UBR+** (*Unspecified Bit Rate+*) - usługa o niezdefiniowanej szybkości bitowej przewidziana dla aplikacji dopuszczających przekaz zgodnie z zasadą „*best effort*” z wyłączeniem funkcji odrzucania komórek. Podobnie jak w usłudze UBR brak jest jakichkolwiek gwarancji dotyczących jakości obsługi. UBR i UBR+ zostały dopasowane do potrzeb wielu tradycyjnych sieci komputerowych LAN i WAN, które generują ruch typu nrt (*non-real-time*) i realizują obsługę typu „*best effort*”. Przykładem może też być sieć Internet, w której protokół datagramowy IP może „gubić” pakietы. Zadaniem protokołu transportowego TCP, w tej sieci, jest zapewnienie integralności i niezawodności przekazu.

**UPC** (*Usage Parameter Control*) - funkcja monitorowania połączenia w sieci ATM, związana z procedurą sprawdzania zgodności deklaracji użytkownika z generowanym przez niego ruchem rzeczywistym. UPC może być realizowana przez algorytm GCRA (*Generic Cell Rate Algorithm*), sprawdzania zgodności komórek, pozwalający na odrzucanie bądź odpowiednie znakowanie ruchu nadmiarowego, generowanego przez użytkownika, przed wprowadzeniem tego ruchu do sieci.

**UTP** (*Unshielded Twisted Pair*) - skrętka nieekranowana, podobnie jak STP, ma postać pary identycznych, izolowanych przewodów umieszczonych we wspólnej osłonie izolacyjnej. Skrętka nieekranowana nie jest chroniona przez ekran, w konsekwencji jest bardziej podatna na zakłócenia zewnętrzne oraz wytwarza wokół siebie stosunkowo duże pole magnetyczne. Podstawową zaletą skrętki nieekranowanej jest niska cena, mały ciężar oraz łatwość instalacji, związana z dużą elastycznością skrętki.

**usługi datagramowe** - usługi przesyłania danych, w których bloki danych (datagramy) są przesyłane przez sieć komunikacyjną między nadawcą a odbiorcą (obiekty warstwy transportowej modelu OSI) bez uprzedniego zestawiania połączenia pomiędzy tymi obiektami. Usługa ta nie daje gwarancji dostarczenia pakietów do miejsca przeznaczenia, możliwy jest też ich odbiór w kolejności innej, od tej, w której zostały nadane.

**usługi izochroniczne** - usługi oparte na transmisjach strumieni izochronicznych, a więc strumieni stawiających ostre wymagania czasowe transmisji danych (wielkość opóźnienia *end-to-end* oraz jego zmienność - tzw. *jitter* i związana z nim szerokość pasma). Usługami izochronicznymi są między innymi usługi multimedialne (videofonia) oraz wszelkiego rodzaju aplikacje czasu rzeczywistego. Aplikacje te wymagają zapewnienia stałej, niezależnej od wielkości ruchu w sieci, szybkości transmisji i zazwyczaj zachowania kolejności przesyłanych pakietów. Transmisje izochroniczne są realizowane głównie przy wykorzystaniu kanałów wirtualnych, gwarantujących odpowiednią przepustowość.

**usługi nazewnicze** - usługi umożliwiające dynamiczną konwersję adresów numerycznych na nazwy (łańcuchy wyrazów i mnemoników) jednoznacznie określające węzły sieciowe. Przykładem usługi nazewniczej jest stosowany w sieci Internet serwis DNS (*Domain Name System*). Jest to rozproszony system baz danych, który tworzy hierarchiczną przestrzeń nazw i umożliwia administratorom podsieci nadawanie stacjom własnych nazw.

**VBR (Variable Bit Rate)** - usługa o zmiennej szybkości bitowej - przewidziana dla źródeł ruchu generujących komórki ze zmienią ale ograniczoną maksymalną intensywnością transmisji i wymagających gwarantowanego poziomu jakości usług. Obecnie usługa ta

jest podzielona na dwa typy: rt-VBR (*real-time Variable Bit Rate*) i nrt-VBR (*non-real-time Variable Bit Rate*).

**WAN (Wide Area Network)** - sieć komputerowa o zasięgu globalnym. Przedstawicielem sieci rozległych jest np. sieć Internet, sieć CompuServe Information Service Network, działająca w USA, czy też sieć Polpak (Polpak-T) działająca w Polsce. Sieci typu WAN oferują bardzo zróżnicowane przepływności w zależności od stosowanej technologii transmisyjnej począwszy od przepływności rzędu kb/s aż do kilkuset Mb/s (155 Mb/s, 622 Mb/s w technice B-ISDN ATM) i pokrywają obszary o promieniu setek a nawet tysiący kilometrów.

**Web serwer** (serwer WWW) - serwer sieciowy pracujący w sieci oferujący usługi WWW. Usługi te są realizowane przez specjalne oprogramowanie aplikacyjne, wykorzystujące protokół HTTP, będący jednym z protokołów warstwy aplikacji w stosie TCP/IP. Web Serwer posiada często możliwość współpracy z innymi aplikacjami przy tworzeniu baz danych, umożliwiając realizację rozproszonych baz danych działających w środowisku sieci TCP/IP.

**wirtualna sieć lokalna (VLAN)** - grupa stacji, znajdujących się w różnych segmentach sieci, które mogą się ze sobą komunikować tak, jakby były w jednej wspólnej sieci lokalnej (odpowiednik domeny rozgłoszeniowej) niezależnie od ich fizycznej lokalizacji. Logiczne grupowanie stacji, niezależnie od ich fizycznej lokalizacji, stało się możliwe po zastosowaniu w sieciach lokalnych technologii przełączania (przełączniki LAN). Komunikacja pomiędzy sieciami wirtualnymi może następować jedynie z wykorzystaniem urządzeń do kierowania ruchem na poziomie warstwy 3 modelu OSI (np. routerów). Istnieje kilka metod realizacji sieci wirtualnych różniących się między sobą sposobem definiowania przynależności stacji końcowych do poszczególnych sieci wirtualnych. Wśród nich możemy wyróżnić trzy główne rozwiązania oparte na grupowaniu: portów (port grouping), adresów MAC (*MAC address grouping*) bądź adresów warstwy 3 modelu OSI (*Layer 3 Based VLANs*).

**WLAN (Wireless LAN)** - bezprzewodowa sieć lokalna wykorzystująca kanał radiowy lub system łączności na podczerwieni jako medium transmisyjne. Podstawowymi standardami bezprzewodowych sieci lokalnych są IEEE 802.11 (stosujący jako podstawowy algorytm dostępu protokół CSMA/CA) oraz opracowany przez ETSI HIPERLAN (*High Performance Radio LAN*) z priorytetową metodą dostępu NPMA łączącą procedury rywalizacji i eliminacji. Standard IEEE 802.11 oferuje usługi: z ograniczeniami czasowymi realizowane za pośrednictwem procedur PCF z punktową koordynacją dostępu do medium oraz usługi asynchroniczne dostępu do kanału implementujące metodę dostępu CSMA/CA, realizowane przez procedury DCF.

**WWW** - usługa sieciowa oferująca uniwersalny serwis informacyjny i przekazywanie informacji. WWW wykorzystuje hipermedialny (hipertekstowy) model organizacji informacji. Działa na zasadzie klient-serwer, opierając się na protokole warstwy aplikacji HTTP.

**wykrywanie i korekcja błędów** - techniki umożliwiające wykrycie i korekcję błędów, pojawiających się w odbieranych blokach lub ciągach danych w wyniku przeklamań i zniekształceń sygnałów, powstających w procesie transmisji danych. W procesie kodowania informacji wyznaczane są nadmiarowe bity kontrolne, pozwalające na detekcję i/lub korekcję błędów wniesionych przez zaszumiony kanał cyfrowy. Podstawową miarą skuteczności stosowanych zabezpieczeń jest tzw. odległość Hamminga określająca minimalną liczbę pozycji, na których różnią się ciągi kodowe danego kodu. Do zabezpieczenia transmisji przed błędami stosowane są głównie blokowe kody liniowe, a wśród

nich kody cykliczne. W cyfrowych systemach telekomunikacyjnych coraz częściej znajdują też zastosowanie kody splotowe. W przypadku wykrycia błędów lub stwierdzenia utraty ramki w warstwie WLD realizowane są algorytmy ARQ retransmisji błędnych lub straconych ramek.

**X.25** - standard CCITT, definiujący zasady współpracy węzła DTE i sieci z komutacją pakietów (rozległej sieci pakietowej). Specyfikacja X.25 jest zbiorem protokołów obejmującym trzy dolne warstwy modelu odniesienia OSI. Oferuje obsługę błędów transmisji oraz sterowanie przepływem ramek (*flow control*), gwarantując stacjom końcowym wiarygodną transmisję. Zapewnia jednakże stosunkowo niewielkie szybkości transmisji.

**X.400** - zalecenie CCITT definiujące system przesyłania wiadomości MHS (Message Handling System) w pakietowej sieci publicznej; stanowi odpowiednik standardu ISO MOTIS (*Message-Oriented Text Interchange Systems*). Analogiczne usługi oferuje protokół SMTP w stosie TCP/IP.

**X.500** - zalecenie CCITT definiujące usługi katalogowe, realizowane w ramach modelu odniesienia ISO OSI. Analogiczne usługi oferuje serwis nazw DNS w architekturze TCP/IP.

**zarządzanie siecią** - proces oraz techniki zdalnego bądź lokalnego konfigurowania oraz monitorowania pracy sieci. Zarządzanie siecią koncentruje się wokół następujących kluczowych zagadnień: zarządzanie konfiguracją, „zarządzanie” awariami, zarządzanie wydajnością, zarządzanie oraz rejestrowanie dostępu do usług, zarządzanie bezpieczeństwem.

**zdalny dostęp do sieci** - dostęp do zasobów sieciowych zlokalizowanych w odległej sieci komputerowej, także przesyłanie danych pomiędzy lokalnym i zdalnym węzłem sieci.