Sieci teleinformatyczne

Na prawach rękopisu
mgr inż. Jacek Jarmakiewicz

SPIS TREŚCI

1 Wstęp

W ostatnich kilkunastu latach sieci komputerowe stały się motorem rozwoju całej współczesnej telekomunikacji. Pierwsze rozwiązania były dedykowane urządzeniom komputerowym (sieć ARPA, Aloha - Stany Zjednoczone). Dążenia projektantów zmierzały do swobodnego transferu informacji pomiędzy programami komputerowymi. Usługi zabezpieczające ten proces, realizowane były w szczególny sposób. O ile urządzenia komputerowe nie realizowały usług uwarunkowanych czasowo i np. nie uczestniczyły w procesach produkcyjnych, gdzie wymagany jest określony czas reakcji - to wymiana wiadomości nawet dużej objętości, nie musiała być realizowana w równych odstępach czasu. Jest to do dzisiaj na ogół cecha, która odróżnia sieci komputerowe od rozwiązań realizujących np. usługę transmisji mowy. Nawet sieci, w których oprócz komputerów mogły znajdować się różnego rodzaju czujniki czy też urządzenia sterujące, tworzące rodzinę sieci telekomunikacyjnych nazywanych lokalnymi, nie były przystosowane do realizacji najstarszej usługi przekazywania mowy na odległość.

Na początek kilka pojąć z zakresu telekomunikacji.

Teleinformatyka - dziedzina, w której pewne systemy telekomunikacyjne są podporządkowane informatyce. Zwykle teleinformatyka służy przesyłaniu informacji pomiędzy komputerami.

Sieci teleinformatyczne - sieci telekomunikacyjne specjalizowane w celu zapewnienia usług wymiany informacji dla systemów informatycznych.

Sieć lokalna - jest siecią telekomunikacyjną, która służy wzajemnemu łączeniu różnorodnych urządzeń wymieniających dane (cyfrowe), rozmieszczonych na niewielkim obszarze.

Urządzenia wymieniające dane to np.:

- komputery;
- terminale;
- urządzenia peryferyjne komputerów;
- czujniki, przetworniki;
- telefony cyfrowe;
- systemy nadzoru;
- alarmowe;
- urządzenia telewizyjne.

Sieć komputerowa - sieć lokalna służąca wzajemnemu łączeniu między sobą komputerów i ich urządzeń peryferyjnych.

Cechy sieci teleinformatycznych w zastosowaniach lokalnych:

- zwykle własność jednego właściciela;
- krótkie odległości (obszar jednego lub kilka budynków);
- zróżnicowana szybkość transmisji - od 50 b/s do do 1 Gb/s;
- niska stopa błędów 10^{-8} do 10^{-11};
- zdecentralizowane sterowanie (mały stopień sprzężenia pomiędzy elementami sieci, przeciwnie do systemów wieloprocesorowych).

Zalety i wady lokalnych sieci teleinformatycznych:

- **zalety:**
  - wspólne wykorzystanie zasobów: urządzeń peryferyjnych, mocy obliczeniowej, pamięci masowej. Dane mogą być gromadzone w sieci w jednym miejscu, ale dostępne są dla wielu użytkowników. Serwery realizują usługi dla wielu użytkowników minimalizując koszty systemu informatycznego przypadające na jednego użytkownika. Zwiększenie efektywności wykorzystania zakupionych urządzeń peryferyjnych - drukarki, skanery itd. tym samym obniżenie kosztów systemu informatycznego dzięki wspólnemu wykorzystywaniu zasobów;
  - podatność systemu na ewolucję, zmiany przyrostowe (w systemach opartych na jednym lub kilku systemach komputerowych, gdy moc obliczeniowa jest skupiona, wszelkie zmiany składu sieci są utrudnione, gdyż zazwyczaj konieczne jest wyłączenie całej instalacji w celu jej przebudowy). Przy rozproszonej mocy obliczeniowej na wiele komputerów sieć może ulegać przebudowie, rozbudowie, ewolucji bez wpływu na resztę dołączonych urządzeń;
  - żywotność, niezawodność (rozproszenie funkcji, redundancja komponentów). Uszkodzenie jednego elementu zazwyczaj nie wpływa na działanie innych elementów sieci. Istnieje możliwość zwiększenia żywotności systemu przez wprowadzenie do sieci elementów redundancyjnych.
  - ułatwienie współpracy użytkowników znajdujących się w różnych pomieszczeniach a realizujących jeden projekt. Tworzenie wirtualnych grup roboczych (z wykorzystaniem odpowiedniego oprogramowania realizującego funkcje warstw wyższych modelu odniesienia);
  - dostęp do wielu komputerów z jednego terminala sieciowego;
  - elastyczność rozmieszczenia elementów wyposażenia.
- **Wady:**
  - brak gwarancji poprawnej współpracy aplikacji i elementów sieci. Jeżeli wykorzystywane są np. różne edytory tekstu to istnieje możliwość, że dokumenty z jednego komputera nie będą „czytane" przez inny, bez konieczności konwersji (format html, pdf, postscript, doc inne). W przypadku braku konwertera lub programu edytującego (czytającego) dokument nigdy nie będzie przeczytany;
  - konieczność rozwiązania problemu integralności baz danych, do których mają dostęp różni użytkownicy próbujący jednocześnie zmieniać dane;
  - konieczność zapewnienie dodatkowego bezpieczeństwa, potrzeba dysponowania mechanizmami obrony przed zniszczeniem lub nieuprawnionym dostępem do informacji sieci teleinformatycznej;
  - trudność w zarządzaniu rozproszonymi zasobami i możliwość utraty kontroli nad zarządzanymi zasobami, użytkownikami.

Obszary zastosowań sieci teleinformatycznych:

- przetwarzanie danych, wiadomości, transfer plików, automatyzacja prac biurowych: edycja tekstów, przetwarzanie dokumentów, opracowywanie informacji, poczta elektroniczna;
- projektowanie, wytwarzanie wspomagane komputerowo;
- inne - systemy bezpieczeństwa, czujniki włamaniowe, alarmowe; realizacja usług telefonicznych, telekonferencyjnych, telewizyjnych.

2 Model odniesienia dla sieci teleinformatycznych

Organizacje standaryzacyjne

Istnieje sześć głównych organizacji standaryzacyjnych, które opracowują standardy dla systemów cyfrowego przesyłania danych. Są to: ISO – Międzynarodowa Organizacja Standaryzacyjna (*ang. International Standards Organization*), CCITT – Międzynarodowa Komisja Konsultacyjna ds. Telegrafii i Telefonii (*ang. International Telegraph and Telephone Consultative Committee*) obecnie ITU – Międzynarodowy Związek Telekomunikacji (*ang. International Telecommunications Union*), EIA – Stowarzyszenie Przemysłu Elektrycznego (*ang. Electrical Industries Association*), ANSI – Amerykański Instytut Normalizacji (*ang. American National Standards Institute*) oraz IEEE – Stowarzyszenie Inżynierów Elektryków i Elektroników (*ang. Institute of Electrical and Electronic Engineers*).

Model RM ISO/OSI

W marcu 1978r ukazał się pierwszy dokument roboczy Międzynarodowej Organizacji Standaryzacyjnej, który prezentował siedmiowarstwową architekturę systemów otwartych. Dokument ten na przestrzeni 6 lat podlegał modyfikacjom i uzupełnieniu, by w roku 1984 stać się standardem międzynarodowym ISO 7498. RM ISO/OSI (*ang. Reference Model for Open system Interconnection - RM ISO/OSI*) przyjęła organizacja CCITT w zaleceniach serii X.200.

Celem międzynarodowego standardu o nazwie Model Odniesienia dla Współdziałania Systemów Otwartych jest dostarczenie wspólnej bazy do koordynowania rozwoju standardów potrzebnych przy pracy nad realizacją współdziałania systemów. Termin Współdziałanie Systemów Otwartych określa standardy przeznaczone do wymiany informacji między systemami. Dzięki obustronnemu stosowaniu odpowiednich standardów są one otwarte wzajemnie dla siebie przy realizacji tej wymiany.

Celem standardu jest także określenie kierunków rozwoju i doskonalenia standardów oraz dostarczanie wspólnego punktu odniesienia w celu utrzymania zgodności wszystkich związanych standardów.

Zalety wprowadzenia standardu:

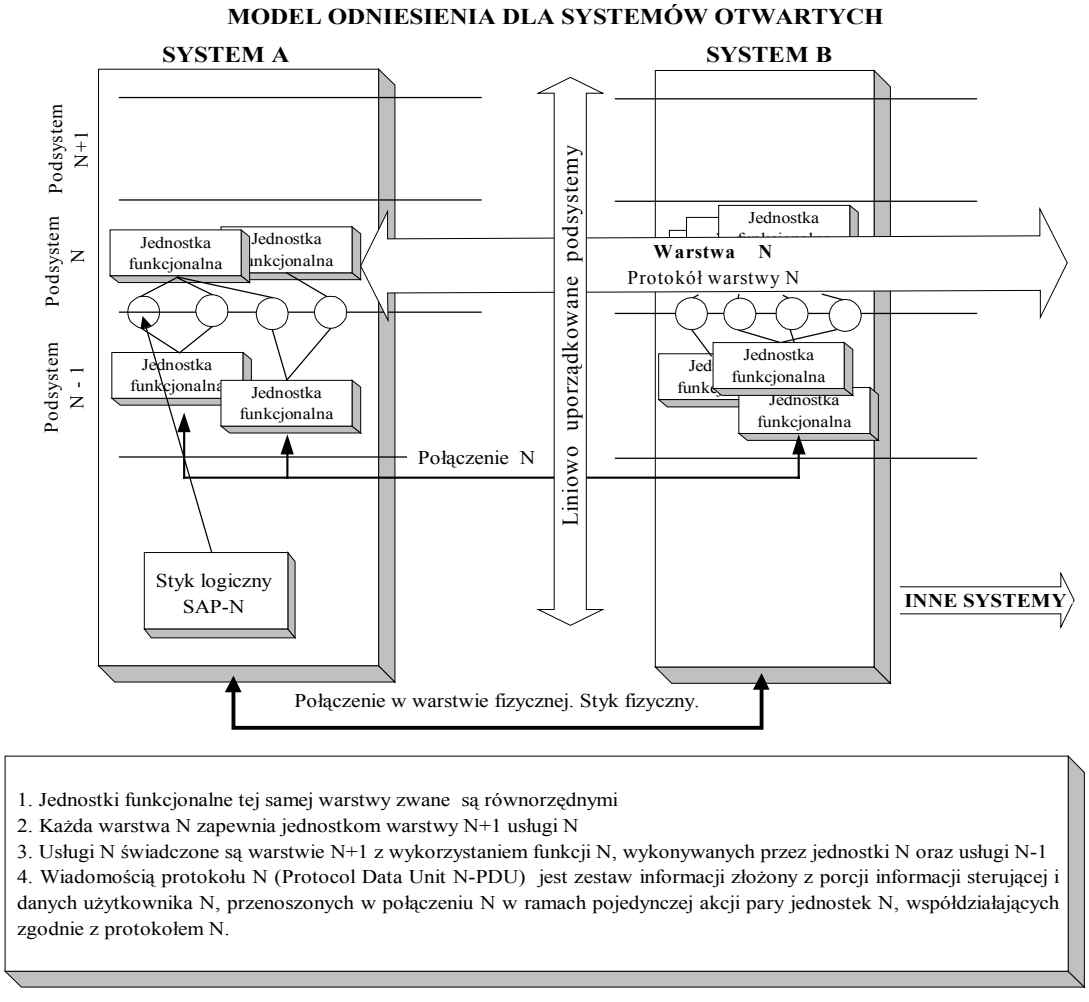
- uporządkowanie rozwoju sieci telekomunikacyjnych;
- uniezależnienie sposobów realizacji procedur warstw modelu;
- zdynamizowanie rozwoju sieci telekomunikacyjnych.

W modelu warstwowym pojedynczy system traktowany jest jako zbiór podsystemów. Systemy w ramach współpracy między sobą wykorzystują podsystemy tego samego rzędu, które tworzą warstwę architektury RM OSI. Z wielu względów okazało się, że optymalnym rozwiązaniem jest przyjęcie siedmiowarstwowej architektury systemu.

W modelu zastosowano technikę strukturalizacji architektury, polegającą na wyróżnieniu warstw funkcjonalnych (*ang. layers*) rysunek 2.1. Zbiór funkcji służących komunikacji pomiędzy systemami otwartymi podzielony został na warstwy, z których każda zawiera odpowiedni podzbiór tych funkcji. Każda warstwa korzysta z usług świadczonych jej przez warstwę niższą, sama świadcząc usługi warstwie wyższej. Szczegóły wewnętrzne każdej warstwy są ukryte przed innymi warstwami, natomiast komunikacja pomiędzy nimi odbywa się przez zdefiniowany styk (*ang. interface*)

funkcjonalny. Styk ten definiowany jest jako zbiór operacji elementarnych (prymitywów) o kilku zaledwie typach:

- N-(nazwa_funkcji).request (żądanie). Warstwa N+1 żąda zainicjowania wykonania danej funkcji w warstwie N;
- N-(nazwa_funkcji).confirmation (potwierdzenie). Warstwa N informuje warstwę N+1 o wynikach wykonania żądanej funkcji (pozytywnym lub negatywnym). W modelu odniesienia dla sieci lokalnych potwierdzenie zwykle dotyczy akcji lokalnych warstwy N (np. przyjęcie danych do nadania), a nie akcji całego łańcucha komunikacji (np. potwierdzenia odebrania danych przez abonenta sieci);
- N-(nazwa_funkcji).indication (zawiadomienie). Warstwa N powiadamia warstwę N+1 o zdarzeniu, które nie wynika bezpośrednio z uprzedniego żądania warstwy wyższej (np. odebrano wiadomość od abonenta sieci);
- N-(nazwa_funkcji).response (odpowiedź). Warstwa (N+1) zawiadamia warstwę N o zakończeniu działań, podjętych w wyniku otrzymania zawiadomienia [N-(nazwa_funkcji).indication].



Rysunek 2.1 Model odniesienia dla systemów otwartych

W modelu OSI system przedstawiony jest jako liniowo uporządkowane podsystemy. Podsystemy tego samego poziomu (cechujące się tą samą funkcją ogólną) tworzą warstwy. Podsystemy składają się z jednostek funkcjonalnych. Jednostki tej samej warstwy zwane są równorzędnymi (*ang. peer*). Każda warstwa N zapewnia

jednostkom warstwy N+1 usługi N (nie dotyczy to warstwy najwyższej). Usługi N świadczone są warstwie N+1 z wykorzystaniem funkcji N, wykorzystywanych przez jednostki N oraz usługi N-1. Usługi N świadczone są jednostkom N+1 w punktach dostępu do usług N (*N-SAP - N ang. Service Access Point*). Które stanowią elementy styku logicznego jednostek N oraz N+1. Podstawową usługą warstwy N, świadczoną na rzecz warstwy N+1, są połączenia N umożliwiające współdziałanie jednostek N+1 w wykonaniu funkcji N+1 (w tym tworzenia połączeń N+1).

W przypadku, gdy pomiędzy systemami istnieje możliwość wymiany informacji, warstwy systemów komunikują się między sobą wykorzystując zdefiniowany wcześniej zbiór reguł i formatów tzw. protokół.

W ramach protokołu są wymieniane:

- informacje sterujące protokołu N, służące koordynacji działania jednostek;
- dane użytkownika N, tj. dane przenoszone pomiędzy jednostkami N w ramach usługi świadczonej przez nie na rzecz jednostek N+1.

Wiadomością protokołu N (*ang. N-Protocol-Data-Unit N-PDU*) jest zestaw informacji złożony z porcji informacji sterującej protokołu N i danych użytkownika N, przenoszonych w połączeniu N w ramach pojedynczej interakcji pary jednostek N, współdziałających zgodnie z protokołem N.

Z punktu widzenia architektury OSI istotne są protokoły N między jednostkami N należącymi do różnych systemów. Jedna jednostka może stosować jeden lub wiele protokołów. Sensowna komunikacja między jednostkami N wymaga zgodnego wyboru jednego protokołu N.

Funkcje spełniane przez warstwy w modelu odniesienia

W modelu OSI zdefiniowano 7 warstw. W związku z obszarem zainteresowań dotyczącym sieci lokalnych szczególny nacisk położono na przedstawienie modelu funkcjonowania trzech dolnych warstw modelu RM OSI. Zostały one opisane poniżej.

Warstwa fizyczna

Obsługuje proces ustanawiania, utrzymywania i rozłączania połączeń fizycznych pomiędzy systemami oraz realizuje funkcje niezbędne do transmisji informacji po takich połączeniach. Transmisja odbywa się w kanale komunikacyjnym, który jest ścieżką komunikacyjną pomiędzy dwoma stacjami warstwy fizycznej w medium fizycznym. Następuje w niej przekształcenie strumienia bitów na sygnały w medium transmisyjnym oraz funkcja odwrotna. Warstwa opisywana jest przez cztery typy charakterystyk:

- charakterystyka mechaniczna (właściwości mechaniczne złącza);
- charakterystyka elektryczna (opisuje wartości przekazywanych z/do medium napięć i prądów oraz ich zmiany w czasie);
- charakterystyka funkcjonalna (opisuje realizowane funkcje przypisując sygnałom określone znaczenie);
- charakterystyka proceduralna (opisuje sekwencje zdarzeń, które muszą zajść aby nastąpiło ustanowienie fizycznego połączenia, utrzymania i transmisja danych oraz rozłączenie).

Usługi i elementy usług dostarczane przez warstwę fizyczną są następujące:

- połączenia fizyczne - transparentna transmisja strumieni bitów pomiędzy stacjami warstwy fizycznej. Połączenie może pozwalać na dupleksową lub półdupleksową transmisję strumieni bitów;

- jednostki danych usług - jeden bit w transmisji szeregowej, "n" w równoległej;
- końcowe punkty połączenia fizycznego - warstwa fizyczna dostarcza identyfikatory punktów końcowych (dwa albo więcej) połączenia fizycznego warstwie liniowej. W ten sposób stacja liniowa identyfikuje kanały komunikacyjne;
- sekwencjonowanie - bity w warstwie fizycznej są obsługiwane w kolejności ich dostarczenia;
- zawiadamianie o błędach - stacje warstwy wyższej są zawiadamiane o uszkodzeniach w warstwie fizycznej;
- parametry jakości usługi - jakość usługi zależy od kanału komunikacyjnego, jest charakteryzowana przez stopę błędu, dostępność usługi, szybkość transmisji, opóźnienie tranzytowe.

Warstwa fizyczna realizuje następujące funkcje:
- uaktywnianie i deaktywacja połączenia fizycznego;
- transmisja jednostki danych połączenia fizycznego;
- zarządzanie warstwą fizyczną (sterowanie w sytuacjach błędnych).

Warstwa łącza danych (liniowa)

Ma za zadanie przekształcić wprowadzający błędy kanał transmisyjny w kanał bez błędów. Na tym poziomie wyróżniane są systemy transmisji synchronicznej i asynchronicznej. Zabezpieczenie przed błędami uzyskiwane jest zazwyczaj przez organizowanie danych w numerowane bloki-ramki, które poddawane są kodowaniu nadmiarowemu (zwykle detekcyjnemu), oraz przekazywanie potwierdzeń poprawnego odbioru ramek, pozwalających ponadto kontrolować szybkość przepływu danych. Typowym standardem obejmującym funkcje warstwy łącza jest protokół HDLC.

Warstwa łącza danych dostarcza środków funkcjonalnych i proceduralnych do ustanawiania, utrzymywania i zwalniania połączeń liniowych między stacjami sieciowymi oraz do transferu jednostek danych usługi liniowej. Połączenia liniowe są tworzone na jednym lub kilku połączeniach fizycznych. Warstwa liniowa wykrywa i w miarę możliwości koryguje błędy, które mogą powstać w warstwie fizycznej. Umożliwia także sterowanie współdziałaniem obwodów danych w warstwie fizycznej.
Usługi i elementy usług dostarczane warstwie sieciowej:
- połączenia liniowe - warstwa liniowa dostarcza jedno lub więcej połączeń liniowych między dwoma stacjami sieciowymi. Połączenie jest zawsze ustanawiane i zwalniane dynamicznie;
- jednostki danych usługi liniowej - warstwa liniowa pozwala na wymianę jednostek danych usługi liniowej na połączeniu liniowym. Jej rozmiar może być ograniczony przez zależność między stopą błędu na połączeniu fizycznym i możliwością wykrywania błędów przez warstwę liniową;
- identyfikatory końcowych punktów połączenia liniowego - punkty końcowe połączenia liniowego mogą być wykorzystane przez stację sieciową do identyfikacji współpracującej z nią stacji sieciowej;
- sekwencjonowanie;
- zawiadamianie o błędzie - błędy wykrywane w warstwie liniowej, których ta warstwa nie może naprawić, są zgłaszane do stacji sieciowej;
- sterowanie przepływem - stacja sieciowa może dynamicznie sterować tempem, w jakim odbiera jednostki danych usługi liniowej z połączenia liniowego;
- parametry jakości usług - warstwa liniowa ustanawia i utrzymuje wybraną jakość usługi w czasie trwania połączenia liniowego. Parametrami jakości usługi są: średni

czas między wykryciem nienaprawialnych błędów, dostępność usługi, opóźnienie tranzytowe i przepustowość, resztkowa stopa błędów, przy czym błędy mogą wynikać ze zmian, utraty lub duplikacji, zaburzenia porządku lub innych przyczyn.

Funkcje realizowane w warstwie liniowej:

- ustanawianie i zwalnianie połączeń liniowych - funkcja ta identyfikuje, ustanawia i zwalnia połączenia liniowe na aktywnych połączeniach fizycznych;
- odwzorowanie jednostek danych usługi liniowej - funkcja odwzorowuje wzajemnie jednoznacznie jednostki danych usługi liniowej na jednostki danych protokołu liniowego;
- rozszczepianie połączenia liniowego - funkcja realizuje rozszczepienie jednego połączenia liniowego na kilka połączeń fizycznych;
- ograniczenia i synchronizacja - funkcja zapewnia rozpoznawanie sekwencji jednostek danych usługi warstwy fizycznej, transmitowanych na połączeniu fizycznym jako jednostki danych protokołu liniowego;
- sterowanie sekwencją - funkcja zachowuje kolejność jednostek danych usługi liniowej przechodzących przez połączenie liniowe;
- wykrywanie błędu - funkcja wykrywa błędy transmisji, formatu i działania występujące na połączeniu fizycznym, albo będące wynikiem złego funkcjonowania współdziałającej stacji liniowej;
- odtwarzanie stanu po błędzie - funkcja próbuje odtworzyć stan po wykryciu błędów transmisji, formatu, działania oraz zawiadamia stacje sieciowe o błędach nienaprawialnych;
- sterowanie przepływem;
- identyfikacja stacji liniowej i wymiana parametru;
- sterowanie współdziałaniem kanału komunikacyjnego - funkcja przenosi zdolność do sterowania współdziałaniem obwodów w warstwie fizycznej do stacji sieciowej;
- zarządzanie warstwą liniową - funkcja uaktywniania i sterowania w sytuacjach błędnych.

Warstwa sieciowa

Zanim zaprezentowane zostaną usługi i funkcje świadczone przez warstwę należy zdefiniować pojęcie podsieci i połączenia w podsieci. Podsieć jest zbiorem składającym się z jednego lub większej ilości pośrednich systemów otwartych, które spełniają rolę przekaźników i przez które końcowe systemy otwarte mogą ustanawiać połączenia sieciowe. Połączenie w podsieci rozumiane jest jako droga komunikacyjna poprzez podsieć, która używana jest przez stację warstwy sieciowej w realizowaniu połączenia sieciowego.

Warstwa sieciowa dostarcza środków do ustanawiania, utrzymania i rozłączenia połączeń sieciowych pomiędzy systemami otwartymi, zawierającymi komunikujące się stacje. Dostarcza również środków funkcjonalnych i proceduralnych do wymiany, przez połączenia sieciowe, jednostek danych usługi sieciowej między stacjami transportowymi. Warstwa sieciowa zapewnia stacjom transportowym niezależność od przyjętych sposobów marszrutyzacji związanych z ustanowieniem i działaniem danego połączenia sieciowego, włączając w to sytuację, gdy stosowanych jest jednocześnie kilka podsieci. Warstwa ta przesłania stacjom transportowym sposób wykorzystania zasobów warstw niższych sieci telekomunikacyjnej w procesie przesyłania informacji.

Podstawową usługą warstwy sieciowej jest zapewnienie przezroczystego transferu danych między stacjami transportowymi. Warstwa sieciowa zawiera funkcje niezbędne

do zamaskowania różnic występujących w charakterystykach różnych rodzajów transmisji i technologii podsieci oraz utworzenia spójnej usługi sieciowej. Jakość usługi jest negocjowana i ustanawiana pomiędzy stacjami transportowymi a stacjami sieciowymi w czasie ustanawiania połączenia sieciowego.
Usługi i elementy usług dostarczane przez warstwę sieciową:
- adresy sieciowe (adresy sieciowe są dostarczane przez warstwę sieciową i są używane przez stacje transportowe do jednoznacznej identyfikacji innych stacji transportowych);
- połączenia sieciowe (połączenie sieciowe dostarcza środków do przesyłania danych pomiędzy stacjami transportowymi, ustanawiania, utrzymania i zwalniania połączeń sieciowych, połączeń pomiędzy dwoma stacjami transportowymi może być kilka);
- identyfikatory punktów końcowych połączenia sieciowego (jednoznacznie definiuje punkt końcowy połączenia sieciowego);
- transfer jednostki danych usługi sieciowej (warstwa sieciowa umożliwia transmisję jednostek danych usługi sieciowej w połączeniu sieciowym);
- parametry jakości usługi (są to: resztkowa stopa błędu, dostępność usługi, niezawodność, przepustowość, opóźnienie tranzytowe, opóźnienie w ustanawianiu połączenia sieciowego);
- zawiadamianie o błędzie (wykrywane błędy nienaprawialne warstwa sieciowa zgłasza do stacji transportowej);
- sekwencjonowanie (warstwa sieciowa może zapewnić sekwencjonowanie informacji jednostek danych usługi sieciowej);
- sterowanie przepływem (może być przekazane do warstwy transportowej);
- przyspieszony transfer jednostek danych usługi sieciowej (warstwa sieciowa może dostarczać dodatkowych środków wymiany informacji);
- zerowanie (likwidowane są wszystkie jednostki informacji będące w trakcie przesyłania, przekazywana jest informacja o zerowaniu do odbiorczej stacji transportowej);
- zwalnianie (stacja transportowa może wymusić zwolnienie połączenia sieciowego w każdej chwili dialogu);
- odbiór potwierdzenia (stacje transportowe mogą wzajemnie potwierdzać odebrane dane).

Zapewnia transmisję bloków danych-pakietów przez sieć komutacyjną po odpowiednio dobranych trasach (zwykle w drodze komutacji łączy albo komutacji pakietów) i dostarczanie ich wskazanym adresatom. Przykładem standardu jest protokół CCiTT X.25.
W warstwie sieciowej realizowane są następujące funkcje:
- marszrutyzacja i funkcje przekaźnikowe;
- połączenia sieciowe;
- multipleksacja połączenia sieciowego;
- segmentacja i blokowanie;
- wykrywanie błędów;
- odtwarzanie stanu po błędzie;
- sekwencjonowanie;
- sterowanie przepływem;
- transfer danych przyspieszonych;
- zerowanie;

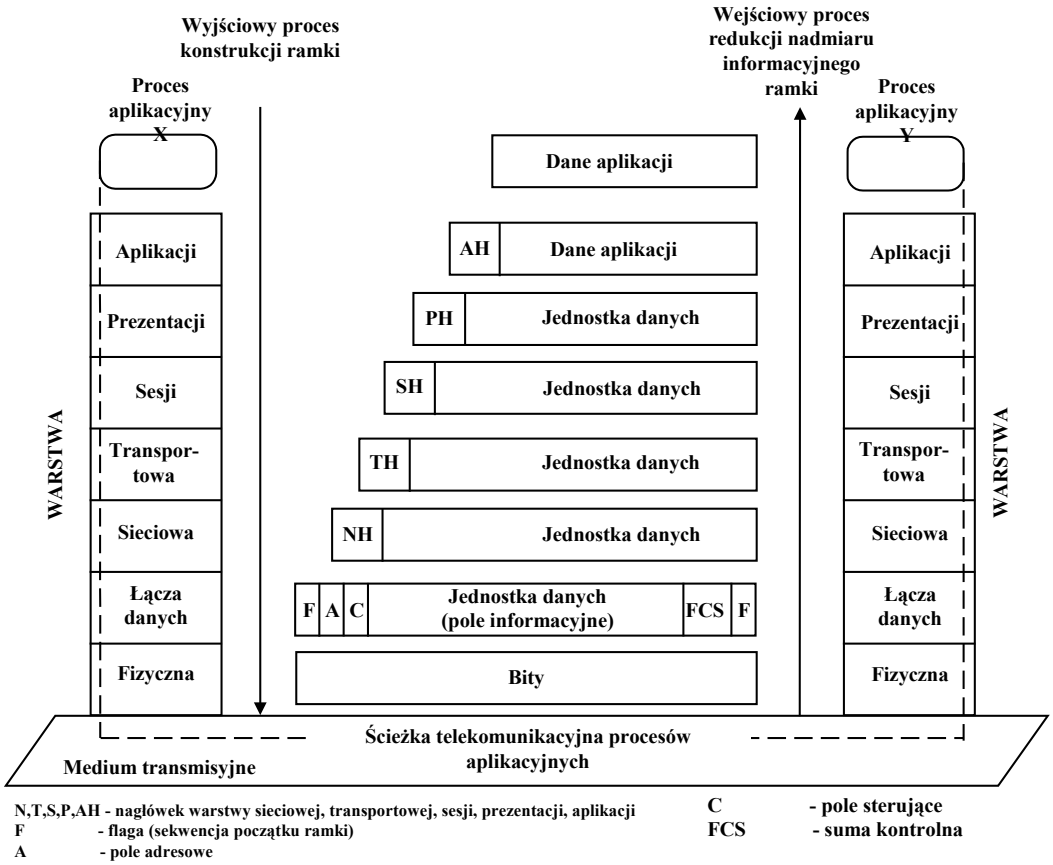
- wybór usługi;
- zarządzanie warstwą.

Warstwa transportowa

Dokonuje podziału wiadomości na bloki (przekształcenia odwrotnego) oraz zapewnia bezbłędne ich przekazywanie między punktami końcowymi (end-to-end) bez ich utraty, duplikacji bądź zmiany kolejności, kontrolując ich priorytety, opóźnienia oraz tajność.

Warstwa sesji

Odpowiada za przebieg dialogu pomiędzy użytkownikami (warstwy wyższe). Określa ona tryb dialogu (przekazywanie danych dwukierunkowe jednoczesne, naprzemienne, jednokierunkowe) momenty przekazywania danych (np. związane z synchronizacją dostępu do wspólnych zasobów), punkty i sposób restartowania itp.



Rysunek 2.2 Proces przesyłania jednostek danych pomiędzy warstwami modelu OSI

Warstwa prezentacji

Dokonuje transformacji kodów i formatów danych stosowanych przez użytkownika na kody i formaty stosowane w sieci (w tym kompresja i utajnianie) i odwrotnie. Protokoły tej warstwy nazywa się czasami terminalami wirtualnymi. Warstwa prezentacji odgrywa szczególną rolę w sieciach heterogenicznych, charakteryzujących się dużą różnorodnością sprzętu i oprogramowania

Warstwa aplikacji (zastosowań)

Świadczy usługi użytkownikom środowiska OSI. Przykładowymi usługami są transfer plików, poczta elektroniczna, obsługa transakcji, utrzymanie sieci.

Przesłanie jednostki danych do partnera dokonuje warstwa aplikacji. Jednak przesłanie to jest wirtualne, jednostka danych jest powierzana kolejnym (niższym) warstwom architektury a fizyczna transmisja między systemami prowadzona jest przez warstwę najniższą fizyczną.

Przekazywane do niższych warstw jednostki uzupełniane są dodatkowymi polami (nagłówki, uzupełnienia) zaś w systemie odbierającym są one odejmowane. Proces ten nazywany jest enkapsulacją. Niestety proces ten prowadzi do dużej redundancji informacyjnej. Przy krótkich wiadomościach długość wiadomości może wzrosnąć pięciokrotnie. Proces ten przedstawiono na rysunku 2.2.

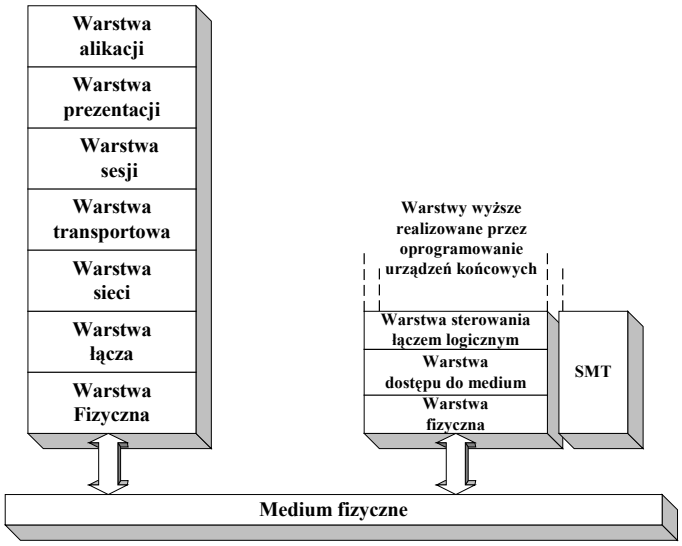
Model odniesienia dla sieci lokalnych

Warstwowy model ISO /OSI powstał z myślą o systemach i sieciach rozległych. W związku z tym jest on z jednej strony dobrym punktem wyjścia do opisu protokołów sieci lokalnych. Jednak z drugiej strony w protokołach sieci lokalnych pojawiają się elementy, które nie występują w sieciach rozległych i co gorsze nie zostały przewidziane w modelu odniesienia OSI.

W sieci lokalnej wszystkie współpracujące stacje dysponują stale połączeniami fizycznymi pomiędzy sobą. Dlatego też w sieciach lokalnych okazały się zbędne funkcje marszrutyzacji i funkcje komutacji wiadomości (wiadomości są rozgłaszane do wszystkich użytkowników sieci lokalnej). Skoro jednak w sieci lokalnej wszystkie stacje mają ze sobą stałe połączenie to istotnym problemem staje się dzielenie wspólnego medium. Konieczna jest realizacja funkcji rozproszonego dostępu do medium.

Funkcje rozproszonego dostępu do medium prezentowane są w modelu odniesienia dla sieci lokalnych przez wprowadzoną, pomiędzy warstwę fizyczną i łącza danych - warstwę dostępu do medium.

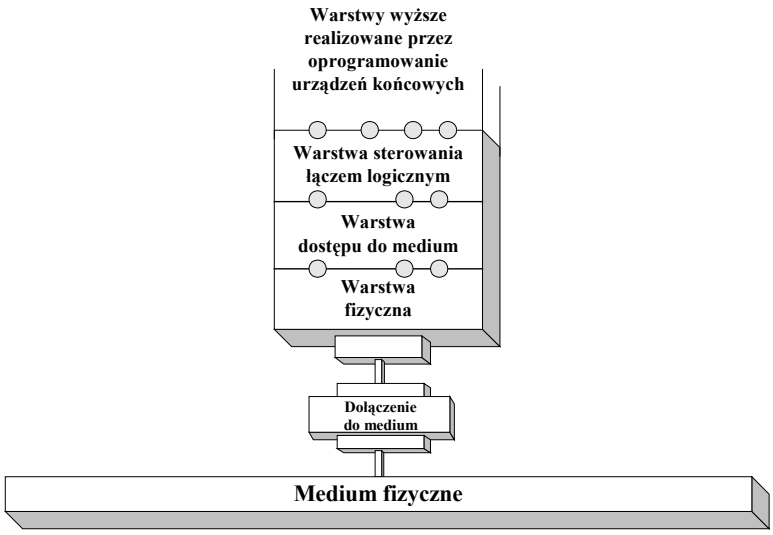
Opracowaniem modelu odniesienia dla sieci lokalnej zajęło się w latach 80 Stowarzyszenie Inżynierów Elektryków i Elektroników. Projekt przyjął nazwę projektu 802 (nawiasem mówiąc jest to data rozpoczęcia projektu luty 1980 roku). Powstały model nosi nazwę modelu odniesienia dla sieci lokalnych i metropolitalnych (*ang. L&M RM Local and Metropolitan Area Reference Model*). Schemat modelu odniesienia dla sieci lokalnej i metropolitalnej na tle modelu RM OSI przedstawiono na rysunku 2.3.



Rysunek 2.3 Warstwowy schemat modelu odniesienia dla sieci lokalnej i metropolitalnej

Model obejmuje dwie najniższe warstwy modelu OSI. W modelu L&M RM LAN wyróżniono następujące warstwy:

- warstwa fizyczna PS (*ang. Phisical Signalling Layer*);
- warstwa sterowania dostępem do medium MAC (*ang. Medium Access Control Layer*);
- warstwa sterowania łączem logicznym LLC (*ang. Logical Link Control Layer*).

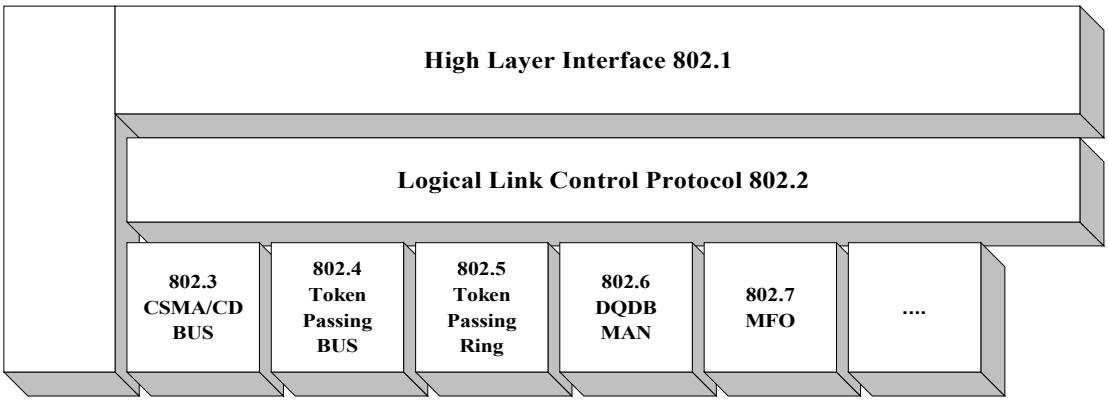


Rysunek 2.4 Implementacyjny model odniesienia dla sieci LAN

Wyróżnia się także warstwę SMT (*ang. Station Management*) jednak w sposób jawny występuje tylko w sieciach z przekazywaniem uprawnienia do nadawania (Token Ring, Token Bus, FDDI).

Chociaż powstały model poprawnie opisuje współdziałanie warstw to często w sposób jawny wyróżniane są fizyczne elementy przyłączeniowe do sieci LAN. Przedstawiono to na modelu implementacyjnym dla sieci LAN na rys. 2.4.

Komisja IEEE 802 opracowała grupę standardów dla wszystkich warstw modelu sieci LAN MAN (rysunku 2.5).



IEEE 802.1 - High Layer Interface
IEEE 802.2 - Logical Link Control
IEEE 802.3 - CSMA/CD Ethernet
IEEE 802.3u - Fast Ethernet
IEEE 802.3z - Gigabit Ethernet
IEEE 802.4 - Token Bus Network
IEEE 802.5 - Token Ring Network
IEEE 802.6 - Metropolitan Area Network
IEEE 802.7 - Broadband Optic Technical Advisory Group
IEEE 802.8 - Fiber Optic Technical Advisory Group
IEEE 802.9 - Integrated Voice and Data LAN Interface
IEEE 802.10 - Standard For Interoperable LAN Security
IEEE 802.11 - CSMA/CA Wireless LAN
IEEE 802.12 - 100VG-AnyLAN

Rysunek 2.5 Struktura komitetu IEEE 802

Protokół sterowania łączem logicznym LLC

Podobnie jak przedstawiono w modelu siedmiowarstwowym RM OSI i tutaj warstwa druga odpowiedzialna jest za zapewnienie bezbłędnej wymiany ramek w ustanowionym połączeniu w warstwie fizycznej. Najpowszechniej wykorzystywanym protokołem warstwy łącza danych jest protokół HDLC. Opracowujący projekt komitet 802 po małych modyfikacja przyjął powyższy schemat także dla sieci LAN. Modyfikacje dotyczyły rozszerzenia możliwości adresacji i ograniczenia liczby opcji protokołu a także dodatkowego zabezpieczenia kodowego przeniesionego do warstwy MAC. Z powodu braku warstwy sieciowej wzmocniona została warstwa transportowa, która tutaj dodatkowo realizuje tworzenie i multipleksację połączeń logicznych i kontrolowanie przepływu danych pomiędzy użytkownikami. Usługi w LLC realizowane mogą być w dwóch trybach połączeniowym (rzadko wykorzystywanym) oraz bezpołączeniowym/datagramowym (tryb bezpołączeniowy może być realizowany z potwierdzeniami albo bez potwierdzeń wysyłanych wiadomości).

W trybie bezpołączeniowym nie jest ustanawiane pomiędzy stacjami połączenie logiczne w przeciwieństwie do trybu połączeniowego. Ponadto różnice dotyczą sterowania przepływem wiadomości, które występuje w trybie z potwierdzaniem.

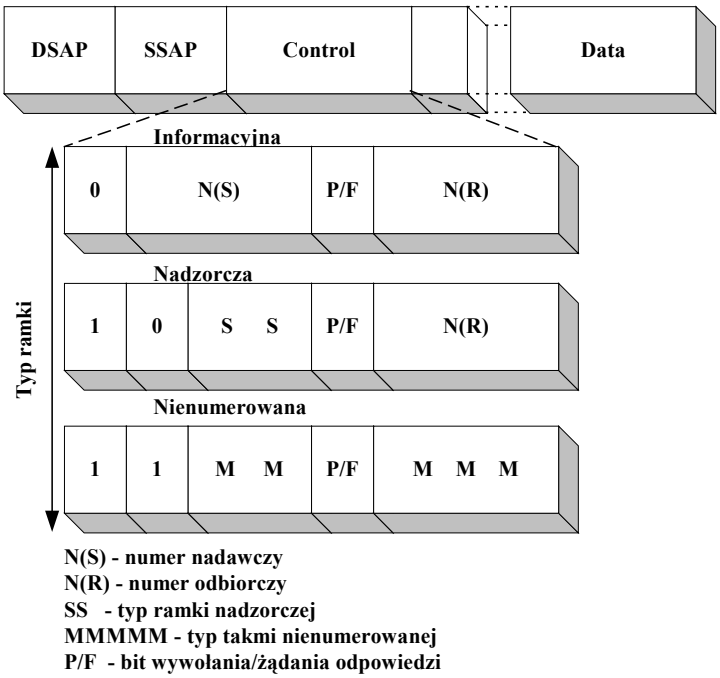
Formaty ramek

Wiadomości przesyłane są pomiędzy punktami dostępu do usług w ramkach zorganizowanych w sposób przedstawiony na rysunku 2.6.

Pola D i SSAP stanowią 7 bitowe adresy punktów dostępu SAP w warstwie LLC, pomiędzy którymi mają być wymieniane wiadomości zawarte w polu danych ramek. Ostatni bit niesiony w oktecie zawierającym adresy w przypadku DSAP niesie informację, czy zawarty adres jest adresem indywidualnym, czy grupowym, a w przypadku SSAP, czy ramka niesie rozkaz, czy odpowiedź na rozkaz. Adresy identyfikujące adresy stacji nadawczej i odbiorczej są niesione w części dołączanej przez warstwę MAC.

Jak można zauważyć, formaty ramek warstwy LLC są identyczne jak w protokole HDLC. Ramki informacyjne służą do wymieniania danych pomiędzy stacjami sieci.

Numery nadawczy i odbiorczy są numerami sekwencyjnymi, które służą celom sterowania przepływem informacji pomiędzy stacjami sieci. W polach tych prowadzona jest numeracja modulo 8. W przypadku nie potwierdzenia siedmiu kolejnych ramek stacja nadawcza zmuszana jest przez stację odbierającą do zaprzestania nadawania kolejnych ramek.



Rysunek 2.6 Format ramki warstwy LLC oraz typy ramek

Ramki nadzorcze wykorzystywane są dla celów potwierdzania i kontroli przepływu danych. Występują trzy typy:

- RR (*ang. Receive Ready*) - gotowość odbioru, ramka używana do potwierdzenia gotowości do odbioru kolejnych ramek informacyjnych;
- RNR (*ang. Receive Not Ready*) - czasowa niegotowość do przyjęcia kolejnych ramek informacyjnych i jednocześnie potwierdzenia odebrania wcześniejszych ramek;
- REJ (*ang. Reject*) - ramka informująca o konieczności powtórzenia ramki z numerem N(R).

Ramki nienumerowane są wykorzystywane do przesyłania danych w trybie bezpołączeniowym oraz do sterowania.

Występują następujące typy ramek:

- komend:
  - SABM - ustanowienie połączenia logicznego;
  - UI - informacja nienumerowana przenosząca nienumerowany blok informacji;
  - DISC - rozłączenie, likwiduje połączenie logiczne;
  - XID - wymiana parametrów pomiędzy stacjami, np. w celu informowania o możliwościach wymiany informacji w trybie połączenia logicznego czy o rozmiarze okna;
  - TEST - żądanie przesłania ramki test w odpowiedzi na identyczną ramkę w celu sprawdzenia LLC.
- odpowiedzi:
  - UA - nienumerowana odpowiedź, potwierdzanie ramek komend SABM, DISC;
  - DM - odłączenie logiczne stacji (disconnect mode);

- FRMR - odrzucenie niepoprawnej ramki w danym stanie (np. ze względów proceduralnych);
- XID odpowiedź na komendę XID;
- TEST - odpowiedź na komendę TEST.

Prymitywy pomiędzy warstwami wyższymi i LLC

Styk pomiędzy warstwami wyższą i niższą jest realizowany z wykorzystaniem odpowiedniego mechanizmu, który posługuje się ściśle określonym zbiorem komend i odpowiedzi, tzw. prymitywami. Warstwa wyższa nie musi wykorzystywać całego zbioru prymitywów. Podzbiór wykorzystywanych prymitywów zależy np. od trybu realizowanego połączenia (tryb połączeniowy i bezpołączeniowy), stanu procesu wymiany danych, potrzeb zarządzania warstwą itp.

Dostęp do usług warstwy LLC odbywa się z wykorzystaniem styku z warstwą wyższą. Wykaz prymitywów dostępnych na styku warstwy wyższe – warstwa LLC przedstawiono w tabeli 2.1.

Tabela 2.1 Prymitywy styku LLC - warstwy wyższe

Usługi bezpołączeniowe bez potwierdzenia	L - RESET.indication
L - DATA.request	L - CONNECTION-FLOWCONTROL.request
L - DATA.indication	L - CONNECTION-FLOWCONTROL.indic..
Usługi bezpołączeniowe z potwierdzaniem	**Usługi zarządzania**
L - DATA-ACK.request	L - SAP-FLOWCONTROL.request
L - DATA-ACK.confirm	L - SAP-FLOWCONTROL.indication
L - DATA-ACK.indication	L - TEST.request
Usługi połączeniowe	L - TEST.indication
L - CONNECT.request	L - STATUS.request
L - CONNECT.confirm	L - STATUS.confirm
L - CONNECT.indication	L - STATUS.indication
L - DATA-CONNECT.request	L - SAP-ACTIVATE.request
L - DATA-CONNECT.confirm	L - SAP-ACTIVATE.confirm
L - DATA-CONNECT.indication	L - SAP-DEACTIVATE.request
L - DISCONNECT.request	L - SAP-DEACTIVATE.confrm
L - DISCONNECT.confirm	L - LAYER-ACTIVATE.request
L - DISCONNECT.indication	L - LAYER-ACTIVATE.confirm
L - RESET.request	L - LAYER-DEACTIVATE.request
L - RESET.confirm	L - LAYER-DEACTIVATE.confirm

Prymitywy między warstwą LLC i MAC

Protokół 802.2 przewidziany jest do współpracy z dowolną warstwą niższą (rysunek 2.5). Specyfikacja tego styku przewiduje zaledwie trzy typy prymitywów:

- MA-DATA.request - żądanie przesłania ramki z lokalnej LLC do LLC w stacji przeznaczenia;
- MA-DATA.confirm - potwierdzenie MAC dla lokalnego LLC, wskazujące przyjęcie lub odrzucenie żądania przez MAC. Potwierdzenie jest istotne lokalnie - nie informuje o dalszych sieciowych losach ramki;
- MA-DATA.indication - przekazuje do lokalnego LLC ramkę odebraną z sieci przez MAC.

Wykaz prymitywów dostępnych na styku warstw MAC i LLC przedstawiono w tabeli 2.2.

Tabela 2.2 Prymitywy styku MAC - LLC

MA-DATA.request	MA-DATA.indication
MA-DATA.confirm	

3 Sieci lokalne

3.1 Ethernet

Zasada działania protokołu dostępu do medium

Terminem CSMA (*ang. Carrier Sense Multiple Access*) oznaczana jest klasa protokołów dostępu losowego, w której przed nadawaniem prowadzony jest nasłuch nośnej a dokładniej analizowana jest aktywność transmisji w medium. Wykrycie ciszy upoważnia do nadawania. W metodzie CSMA wykorzystywany jest poniższy algorytm:

- stacja prowadzi nasłuch informacji w medium;
- jeżeli w medium panuje cisza, to stacja rozpoczyna nadawanie własnych wiadomości;
- jeżeli w medium inna stacja prowadzi wymianę danych, to stacja postępuje zgodnie z jednym z algorytmów:
  - non-persident (stacja nieśmiała) stacja odczekuje kwant czasu i ponawia próbę nadawania. Przy takim algorytmie pozostaje niewykorzystany czas po zakończeniu nadawania stacji aktywnej;
  - 1-persident (stacja zachłanna) stacja po stwierdzeniu zakończenia transmisji przez stację aktywną natychmiast zaczyna nadawać. Jeżeli oczekujących stacji jest kilka, wtedy wystąpi z prawdopodobieństwem równym 1 kolizja, a stacje zostaną rozdzielone w dalszej fazie aktywności. Następuje strata czasu niewykorzystania medium związana z czasem transmisji ramki w medium powiększona o czas okna kolizji;
  - p-persident (stacja sprytna), jeżeli medium jest wolne, stacja nadaje z prawdopodobieństwem równym p., a wstrzymuje się na określony czas (np. czas propagacji t) z prawdopodobieństwem (1-p). W przypadku zajętości medium, stacja kontynuuje nasłuch do czasu zwolnienia medium i postępuje jak opisano wyżej. Straty czasu podobne jak powyżej. Jeżeli w sieci występuje N stacji to w przypadku, gdy $N*p>1$ kolizja wystąpi z prawdopodobieństwem 1. Można oczywiście zmniejszać p, ale wtedy rosną opóźnienia nadawania ramek.
- jeżeli po określonym czasie stacja nie odbierze ramki potwierdzenia, to wnioskuje, że nastąpiła kolizja i ponawia nadawanie ramki po losowo określonym kwancie czasu o nazwie *ang. backoff*.

Algorytm działania sieci opartej na metodzie dostępu CSMA/CD (*ang. Carrier Sense Multiple Access with Collision Detection*) przedstawiono poniżej:

- stacja prowadzi nasłuch informacji w medium;
- jeżeli w medium panuje cisza, to stacja rozpoczyna nadawanie własnych wiadomości;
- równolegle do wysyłania wiadomości do medium stacja prowadzi nasłuch. Jeżeli występuje rozbieżność pomiędzy ramką nadawaną i odbieraną (z nasłuchu, wtedy następuje stwierdzenia faktu kolizji.

– w przypadku wykrycia kolizji stacja przestaje nadawać własna ramkę i zaczyna nadawać krótki sygnał służbowy (jam), zadaniem jego jest poinformowanie stacji sąsiednich o wystąpieniu kolizji. Następnie stacja odczekuje losowy kwant czasu (*ang. backoff*) i ponawia próbę nadawania.

W sieci IEEE 802.3 transmisja sygnału realizowana jest we wszystkich kierunkach w sieci. Jeżeli jedna ze stacji nadaje ramkę, to wszystkie stacje dołączone do medium odbiorą sygnał z opóźnieniem (w związku z faktem skończonej prędkości propagacji sygnału elektrycznego). Na odcinku L maksymalne opóźnienie propagacyjne pomiędzy dwoma najdalej oddalonymi punktami wyniesie:

$$t[s] = \frac{L[m]}{2*10^8[m/s]}$$

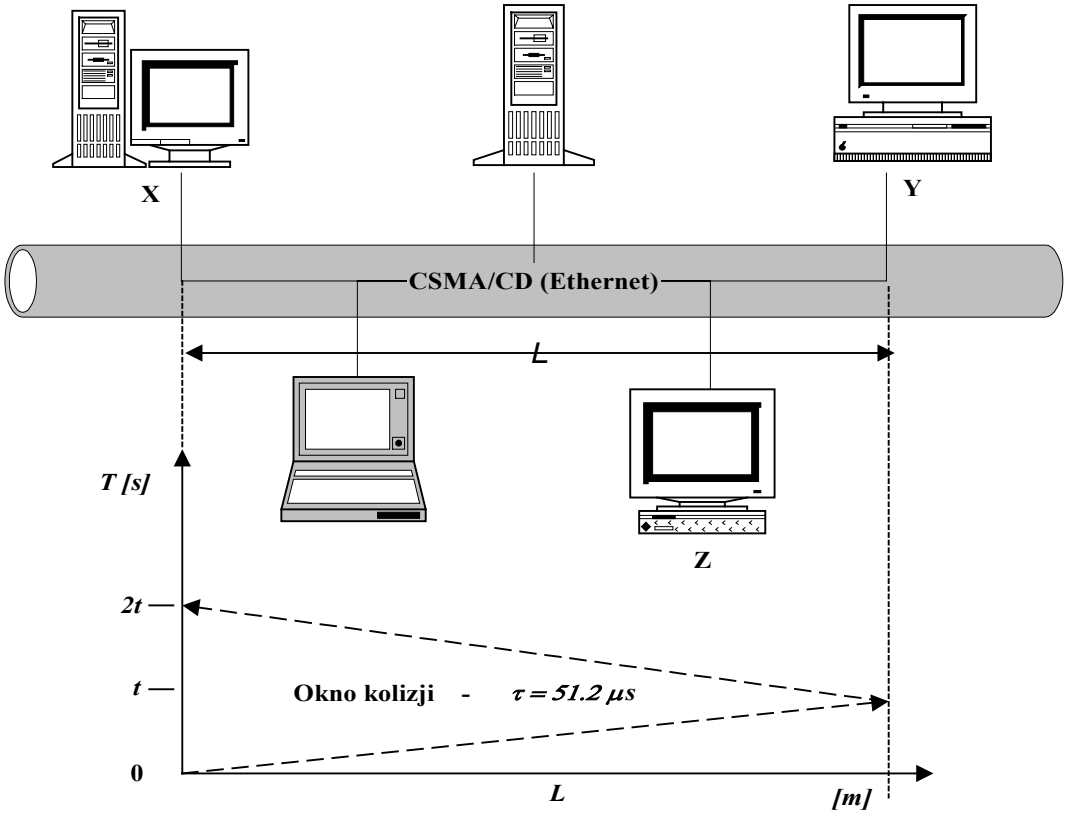
gdzie $2*10^8$ m/s oznacza prędkość rozchodzenia się fali elektromagnetycznej w medium.

Rozpatrzmy przykład

Dwie najdalej oddalone od siebie stacje, na podstawie ciszy stwierdzonej w medium, zaczynają nadawać ramkę. Stacja X rozpoczyna nadawanie. Zanim sygnał od stacji X, dotrze po czasie t do stacji Y, stacja Y zaczyna nadawać. Już po chwili stwierdza kolizję, jednak sygnał nadawany ze stacji Y jest propagowany już w medium, dotrze on do stacji X po czasie także równym t. Dlatego też stacja X wykryje kolizję po czasie:

$$\tau = 2t$$

Czas τ określamy nazwą okna kolizji. Interpretację graficzną przykładu przedstawiono na rysunku 3.1.



Rysunek 3.1 Interpretacja graficzna okna kolizji

Czas oczekiwania na ponowienie transmisji - backoff

W celu poprawy stabilności sieci, w metodzie losowego dostępu do medium z rozstrzyganiem kolizji stosuje się każdorazowe podwojenie długości przedziału losowania czasu oczekiwania po każdym nieudanym ponowieniu nadawania ramki (*ang. binary expotential backoff*). Ponowienia nadawania ramek występuję coraz rzadziej, zmniejszane jest więc chwilowe obciążenie sieci umożliwiając tym samym nadawanie ramek innym stacjom. Działanie takie prowadzi do modelu obsługi kolejki LIFO, tzn. prawdopodobieństwo dotarcia do abonenta ramki ponawianej jest mniejsze niż prawdopodobieństwo dostarczenia ramki nowej, wygenerowanej przez inną stację.
Parametry protokołu IEEE 802.3 - CSMA/CD:

- Szybkość transmisji 10 Mb/s;
- Maksymalna odległość dwóch stacji 2500m;
- Maksymalna długość segmentu 500m;
- Kodowanie transmisyjne Manchester (50% wydajności);
- Media transmisyjne: kabel koncentryczny gruby i cienki - 50 Ohm, skrętka od 3 do 5 kategorii (UTP, STP);
- Okno kolizji 51.2 μs;
- Wykrywanie kolizji następuje po stwierdzeniu poziomu sygnału większego, niż to zapewnia własny nadajnik (w systemie transmisyjnym);
- Minimalna długość ramki 72 bajty;
- Maksymalna długość ramki 1526 bajtów;
- Długość pola danych 46 do 1500 bajtów;
- Maksymalna liczba stacji w sieci 1024;
- Maksymalna liczba stacji w segmencie 100.

Format ramki warstwy MAC

Ogólna budowa ramki warstwy MAC została opracowana przez firmę Digital z udziałem firm INTEL i XEROX i po drobnych zmianach stała się przedmiotem standardu IEEE 802.3

Część początkowa ramki - preambuła - składa się z sekwencji 8 oktetów. Pierwszych siedem oktetów zawiera naprzemienny ciąg zer i jedynek. W ósmym zaś dwa ostatnie bity są jedynkami. Oktet ten nosi nazwę granicy początkowej ramki SFD (*ang. Start Frame Delimiter*). Zadaniem preambuły jest zapewnienie synchronizacji odbiorników stacji przyłączonych do sieci oraz określenie momentu początkowego ramki.

Następne 6-oktetowe pole reprezentuje adres stacji przeznaczenia ramki. Adresem przeznaczenia może być grupa stacji sieci. Taki adres nazywany jest adresem grupowym (*ang. Multicast Address*). Jeżeli ostatni bit (najmniej znaczący) pierwszego oktetu pola adresowego równy jest 1, wtedy adres jest adresem grupowym, gdy zaś równy jest 0, adres jest adresem indywidualnym stacji sieciowej. Ponadto, jeżeli 7-oktetowy adres zawiera same jedynki, wtedy jest to adres rozgłoszeniowy (*ang. Broadcast address*).

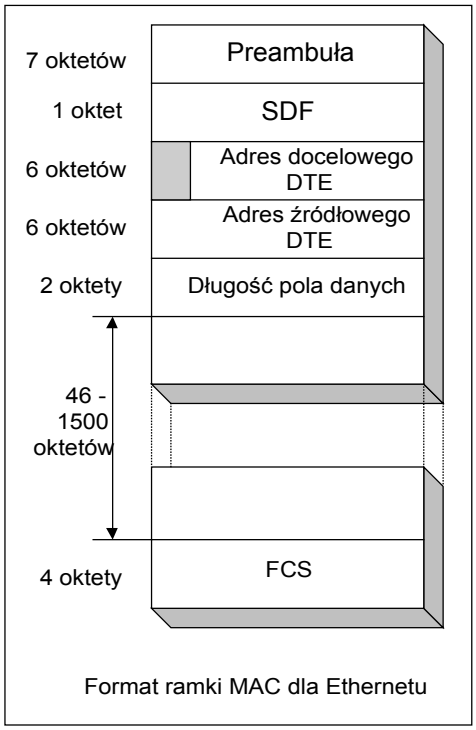
Pole następne jest polem adresowym źródła o długości 6 oktetów. Dwa następne oktety zawierają informacje na temat długości pola danych. Jeżeli pole danych jest krótsze od minimalnego (wymóg by ramka nie była krótsza niż 72 oktety), wtedy pole danych jest sztucznie wypełniane (*ang. padding*). Na podstawie zawartych informacji pomiędzy polami adresu źródłowego i ostatnim oktetem pola danych, wyliczana jest 4

oktetowa suma kontrolna FCS (*ang. Frame Redundancy Checksum*). Format ramki przedstawiono na rysunku 3.2.

Wydajność protokołu

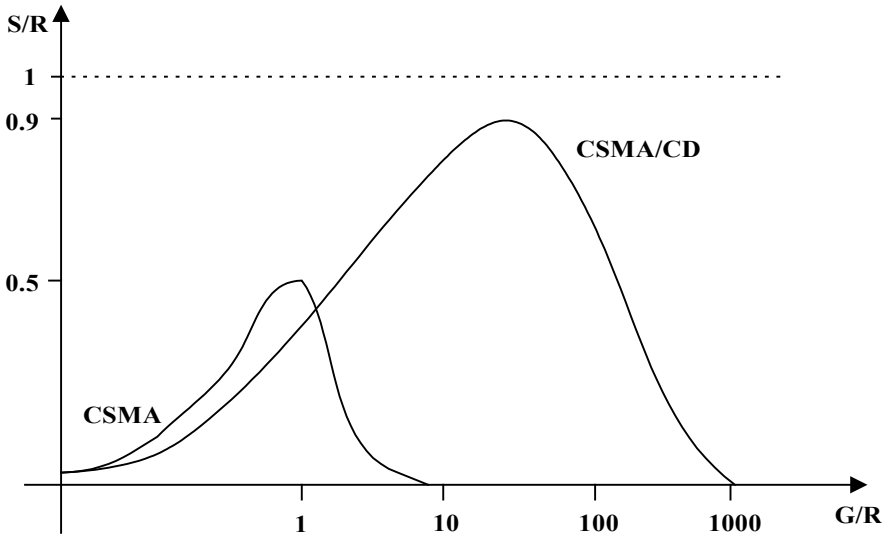
Intuicyjnie można przewidzieć, że w protokole z metodą dostępu opisaną zaleceniem IEEE 802.3:

- poprawna praca jest możliwa tylko przy niewielkim natężeniu przesyłanych ramek, wzrost tego natężenia może prowadzić nawet do zablokowania łącza przez uporczywie pojawiające się kolizje;
- w związku z pojawianiem się kolizji efektywność wykorzystania łącza jest ograniczona i jest mniejsza od przepustowości sieci.



Rysunek 3.2 Format ramki warstwy MAC dla metody IEEE 802.3

Podstawową charakterystyką efektywności rywalizacyjnych protokołów dostępu jest zależność ilości skutecznie przesłanej informacji S w funkcji ilości G informacji zleconej do przesłania (łącznie z retransmisjami spowodowanymi przez kolizje). Szkic takiej zależności przedstawiono na rysunku 3.3.



Zależność ilości *S* skutecznie przesłanej informacji do łącznej ilości *G* informacji zleconej do przesłania. *G* zawiera również informacje retransmitowane. Wartości *S* i *G* wyrażono w postaci wielokrotności szybkości transmisji.

Rysunek 3.3 Zależność ilości skutecznie przesłanej informacji *S* w funkcji ilości *G* informacji zleconej do przesłania

Wykresy zachowują charakterystyczny kształt wskazujący tzw. zjawisko niestabilności. Przekroczenie przez G pewnej wartości krytycznej powoduje zmniejszenie ilości skutecznie przesłanej informacji, a w rezultacie wręcz zablokowanie łącza przez powtarzające się kolizje.

Typy sieci w standardzie Ethernet 10Mb/s

Typy sieci należy rozumieć jako ważniejsze rodzaje ich topologii i technologii budowy. W śród wielu rozwiązań największą liczbę zastosowań znalazły trzy typy sieci Ethernet:

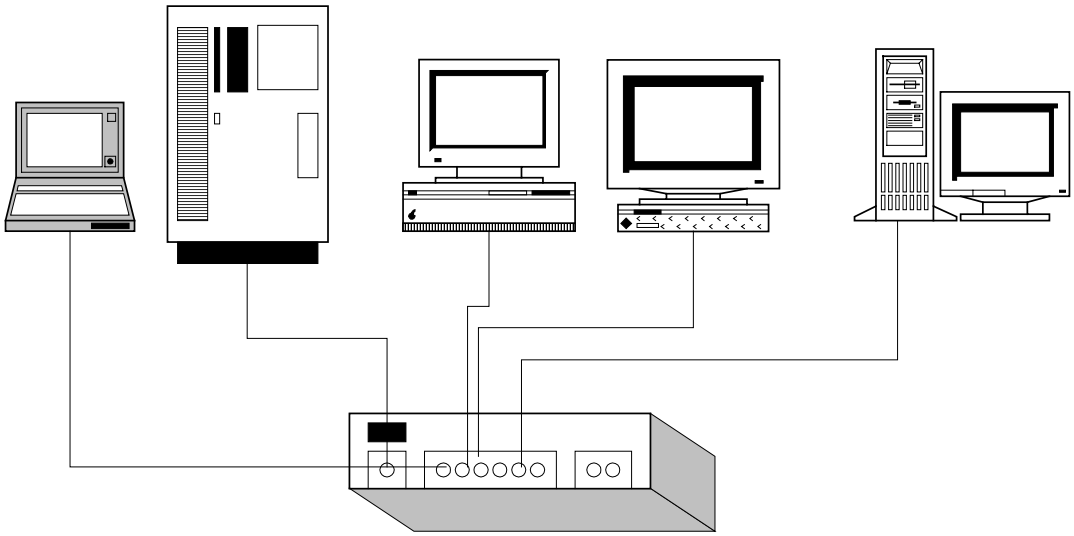
- Ethernet 10BASE T topologia gwiazdy z punktem centralnym w postaci huba kabel skrętka (miedziany);
- ThickNet Ethernet 10BASE 5 (tzw. gruby Ethernet średnica kabla koncentrycznego Φ=0.5 cala, maksymalna długość segmentu 500 metrów);
- ThinNet Ethernet 10BASE 2 (tzw. cienki Ethernet średnica kabla koncentrycznego Φ=0.25 cala, maksymalna długość segmentu 200 metrów);
- Ethernet 10BASE F topologia gwiazdy z punktem centralnym w postaci huba, kabel optyczny (światłowód). Poniżej omówiono poszczególne z nich.

Ethernet 10BASE-T

Sieć Ethernet 10 BASE-T budowana jest w oparciu o medium nazywane popularnie skrętką. Szybkość transmisji 10Mb/s. Jest to kabel 8- żyłowy, którego poszczególne żyły, tworzące pary, zostały ze sobą skręcone. Maksymalna wielkość segmentu sieci lokalnej stworzona w oparciu o to rozwiązanie to 100m. Maksymalna długość sieci składającej się z segmentów to 2500 metrów. Wyróżniamy kilka typów kabli. Najważniejszy podział wyróżnia kable nieekranowane UTP (*ang. Unshielded Twisted Pair Cable*) i ekranowane STP (*ang. Shielded Twisted Pair Cable*). Ponadto rozróżniane są klasy (kategorie kabla), najprościej ujmując w oparciu o kable do kategorii 3 włącznie, można prowadzić transmisję z szybkością do 10Mb/s (w

pojedynczej parze), kable kategorii 4 i 5 mogą przenosić sygnały elektryczne o modulacji 100 i więcej Mb/s.

Topologia. Fizycznie sieć 10Base-T jest gwiazdą z punktem centralnym w postaci huba, logicznie zaś jest magistralą. Hub jest to urządzenie pozwalające łączyć ze sobą poszczególne stacje sieci, pełni rolę inteligentnego złącza. Inteligentnego, ponieważ w przypadku uszkodzenia którejś ze stacji, odłącza ją od sieci i zapewnia nieprzerwaną pracę pozostałej części sieci. Stacja uszkodzona jest separowana od reszty sieci i nie wpływa na jej pracę. W nowoczesnych rozwiązaniach do budowy okablowania sieci wykorzystywany jest kabel nieekranowany 5 klasy (UTP-5).

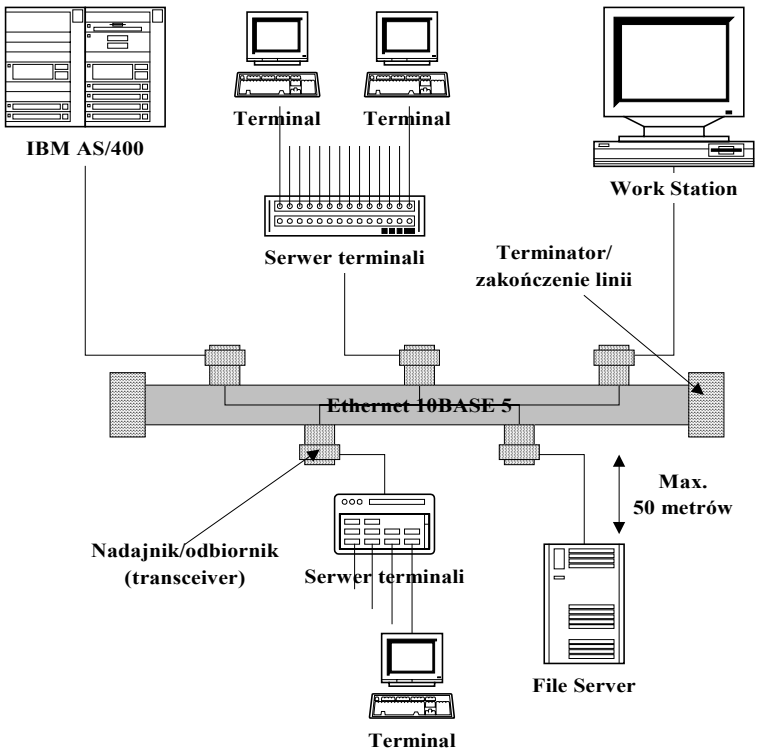


Rysunek 3.4 Przykład sieci Ethernet 10BASE T

Obecnie najpopularniejszym rozwiązaniem jest technika oparta o styk fizyczny RJ-45 (wtyczka i gniazdo podobne do nowoczesnych złączy przy aparatach telefonicznych). Zwykle huby posiadają także możliwość podłączania do nich urządzeń na styku AUI, czy też poprzez złącze BNC. Huby mogą być łączone z sąsiednimi hubami zwiększając tym samym rozmiary sieci. Jednak parametry protokołu przytoczone powyżej nie ulegają zmianie (należy pamiętać, że sieci nie można rozbudowywać w nieskończoność, co jest związane z oknem kolizji). Przykład sieci opartej o typ 10Base-T przedstawiono graficznie na rysunku 3.4.

Ethernet 10BASE 5

Sieć Ethernet 10BASE 5 budowana jest w oparciu o medium kabel koncentryczny 50 Omowy (jak wskazuje nazwa angielska sieci, jest to „gruby" kabel koncentryczny). Szybkość transmisji 10Mb/s. Jego parametry pozwalają na wydłużenie segmentu do 500 metrów. Stacje sieci dołączane są do sieci z wykorzystaniem transceiverów (nadajnik/odbiornik) bezpośrednio do kabla koncentrycznego Długość kabla transceivera (kabel pomiędzy transceiverem a stacją sieci) 50 metrów. Minimalna odległość pomiędzy przyłączonymi transceiverami 2.5 metra. W segmencie nie może występować więcej jak 100 transceiverów. Kabel koncentryczny zakończony jest na końcach terminatorami o rezystancji 50 omów. Przykład sieci opartej o typ 10Base5 przedstawiono graficznie na rysunku 3.5.



Rysunku 3.5 Przykład sieci Ethernet 10BASE5

Topologia. Topologicznie sieć oparta o standard Ethernet - 10BASE-T jest magistralą. Wszystkie stacje sieci podłączone są do kabla koncentrycznego. Całkowita długość sieci (z wykorzystaniem urządzeń wzmacniających repeaterów) 2500 metrów. Przyłącza wewnętrznych kart komputerowych oparte są o standard DB-15 AUI.

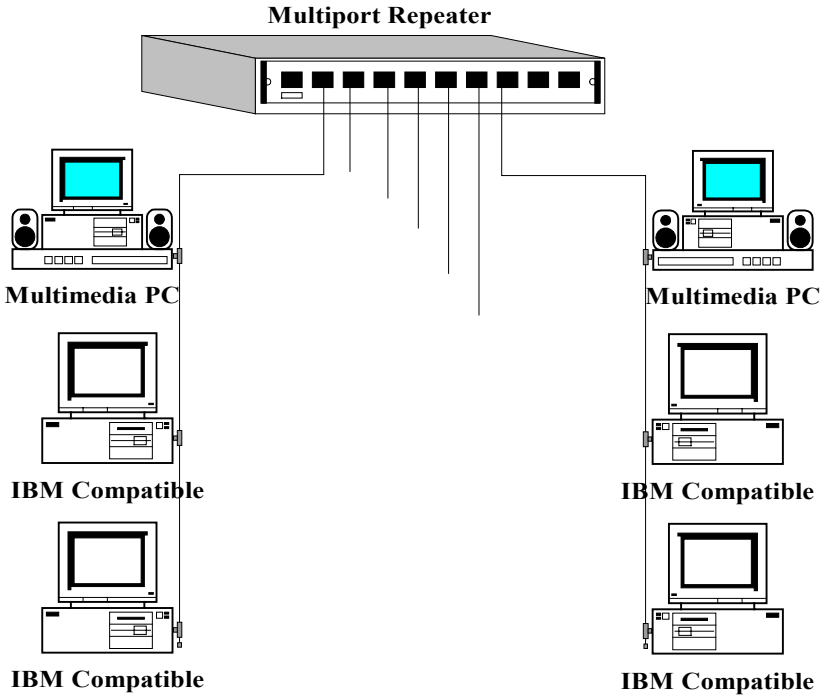
Tego typu topologia była bardzo rozpowszechniona w czasach, gdy ceny hubów i koncentratorów dla sieci LAN były bardzo wysokie. Sieć charakteryzowała się dużą efektywnością ekonomiczną. Jednak obecnie z powodu jej małej żywotności (i obniżenia cen hubów) rozwiązanie nie jest preferowane. Niska żywotność tego typu rozwiązania wynika z faktu awarii całego segmentu sieci w przypadku uszkodzenia (bądź zwarcia) kabla koncentrycznego.

,

Ethernet 10BASE 2

Sieć Ethernet 10BASE 2 zbudowana jest w oparciu o medium kabel koncentryczny 50 omowy (jak wskazuje nazwa angielska sieci, jest to „cienki" kabel koncentryczny). Szybkość transmisji 10Mb/s. Jego parametry pozwalają na budowę segmentu maksymalnie do długości 185 metrów. Stacje sieci dołączane są do sieci z wykorzystaniem T-złączy BNC. Przyłącza te występują bezpośrednio w karcie ethernetowskiej stacji sieciowej, tak więc nie jest wykorzystywany żaden kabel pomiędzy kartą a T-złączem. Jeżeli do przyłączenia używany jest trancsceiver BNC, to maksymalna długość takiego odcinka wynosi 50 metrów.

Minimalna odległość pomiędzy przyłączonymi T-złączami 0.5 metra. W segmencie nie może występować więcej niż 30 przyłączeń. Kabel koncentryczny zakończony jest na końcu terminatorem o rezystancji 50 omów. Przykład sieci opartej o typ 10Base 2 przedstawiono graficznie na rysunku 3.6.



Rysunek 3.6 Przykład sieci Ethernet 10BASE2

Topologia. Topologicznie sieć oparta o standard Ethernet - 10BASE-T jest magistralą. Stacje sieci podłączone są do kabla koncentrycznego, a takie odcinki spinane są między sobą wieloportowym wzmacniaczem (Multiport Repeater). Całkowita długość sieci (z wykorzystaniem urządzeń wzmacniających repeaterów) 925 metrów. Przyłącza wewnętrznych kart komputerowych oparte są na standardzie BNC.

W tabeli 3.1 przedstawiono zbiorcze informacje o typach realizowanych sieci Ethernet.

Tabela 3.1 Parametry sieci Ethernet

Parametr	10BASE5	10BASE2	10BASE-T
Powszechna nazwa	Standardowy lub „gruby” Ethernet	Thinnet, „cienki” Ethernet, Cheapernet	Ethernet oparty na skrętce
Szybkość transmisji	10 Mb/s	10 Mb/s	10 Mb/s
Maksymalna długość segmentu	500 m	200 m	100 m
Maksymalna ilość węzłów w segmencie	100	30	3
Maksymalna ilość repeaterów	2	4	4
Maksymalna ilość węzłów w sieci	1024	1024	N/A
Minimalna odległość między węzłami	2,5 m	0,5 m	Bez ograniczeń
Maksymalna ilość połączonych segmentów	3	3	N/A
Położenie elektroniki transceivera	W złączu kablowym	Scalony z węzłem	Wewnątrz huba
Typowy typ kabla	RG-50 (średnica 0,5 cali)	RG-6 (średnica 0,25 cali)	Nieekranowana skrętka
Typ złącza	Typu N	BNC	RJ-45/Telco
Impedancja kabla	50 Ω	50 Ω	100 Ω
Złącze transceiver - kabel	Typu DB 15 pinowy	BNC	N/A

Ethernet 10BASE-F

Ethernet 10BASE F topologia gwiazdy z punktem centralnym w postaci huba, kabel optyczny (światłowód). Sieć Ethernet 10 BASE-F budowana jest w oparciu o światłowód jedno lub wielomodowy (w zależności od typu kabla uzyskuje się różne odległości pomiędzy stacjami od nawet do 2000 metrów). Ogólnie możemy wyróżnić trzy przypadki sieci oparte na światłowodzie:

- 10 BASE-FL, odległość pomiędzy stacjami wzmacniającymi sygnał może wynosić maksymalnie do 2000 metrów.
- 10 BASE-FB, połączenia realizowane są pomiędzy stacjami wzmacniającymi sygnał, odcinek światłowodowy o długości 2000m;
- 10 BASE-FP, stacje sieci łączone są do wspólnego huba, odcinek pomiędzy stacją a hubem maksymalnie 500m. Topologia sieci 10 BASE FB - gwiazda pasywna. Interpretacja graficzna podobna jest do tej z rysunku 3.4.

Technologię światłowodową wykorzystuje się w przypadku:

- gdy konieczne jest połączenie odległych punktów sieci ze sobą, a ze względu na opóźnienia propagacji sygnału w kablach miedzianych przekroczyłyby okno kolizji;
- w celu podwyższenia bezpieczeństwa sieci;
- przygotowania się do ewentualnej zmiany technologii na szybki Ethernet.

Ethernet 100 Mb/s

W czasie, gdy wielu użytkowników uruchomi jakieś aplikacje multimedialne, standardowy Ethernet 10 Mb/s nie działa zbyt poprawnie. Udoskonaleniem standardowego Ethernetu są dwie sieci: Fast Ethernet oraz 100VG-AnyLAN. Odpowiednimi standardami IEEE dla tych sieci są: dla Fast Ethernetu – IEEE 802.3u oraz 802.12 dla 100VG-AnyLAN. Oba standardy wykorzystywane są w wielu produktach, które umożliwiają szybkość transmisji równą 100 Mb/s. Poprawiają one skuteczność działania sieci przynajmniej 10 razy.

Podstawowymi typami standardów opierających się na Ethernecie 100 Mb/s, które stają się coraz bardziej popularne są:

- 100BASE-TX (skrętka);
- 10BASE-T4 (skrętka);
- 100VG-Any LAN (skrętka);
- 100BASE-FX (kabel koncentryczny).

Fast Ethernet lub inaczej 100BASE-T, jest po prostu zwykłą siecią 10BASE-T pracującą z dziesięć razy szybszym przesyłaniem danych. Przejście od standardowego Ethernetu do jego szybszej odmiany jest rzeczą naturalną i pozwala na łatwą modyfikację sieci. Niestety, podobnie jak w standardowym Ethernecie, węzły rywalizują ze sobą o dostęp do sieci, co zmniejsza jej skuteczność, zwłaszcza w czasie zwiększonego ruchu. Ponieważ, w sieci wykorzystywana jest metoda detekcji kolizji, maksymalna długość segmentu ograniczona jest przez czas, w którym najdalej położone węzły potrafią tą kolizję wykryć. Dla sieci Fast Ethernet wykorzystującej skrętkę miedzianą długość segmentu ograniczona jest do 100 m, a w przypadku kabla światłowodowego do 400 m. Podstawowe parametry sieci Fast Ethernet przedstawione są w tabeli 3.2.

Tabela 3.2 Parametry sieci Fast Ethernet

	100BASE-TX	100VG-AnyLAN
Standard	IEEE 802.3u	IEEE 802.12
Szybkość transmisji	100 Mb/s	100 Mb/s
Rzeczywista przepustowość	Do 50 Mb/s	96 Mb/s
Maksymalna odległość (hub – węzeł)	100 m (skrętka, Kategoria 5) 400 m (światłowód)	100 m (skrętka, Kategoria 3) 200 m (skrętka, Kategoria 5) 2 km (światłowód)
Możliwość unowocześnienia	Brak	Do 400 Mb/s
Zalety	Łatwa migracja z 10 BASE-T	Większa przepustowość, większa odległość

Ponieważ standardy sieciowe 100BASE-T i 10BASE-T są wzajemnie kompatybilne, sieć pozwala na transmisję danych z szybkością zarówno 10 Mb/s, jak i 100 Mb/s. Zatem węzły umożliwiające transmisję 100 Mb/s, mogą się również komunikować z węzłami o mniejszej szybkości transmisji (10 Mb/s).

Standard 100VG-AnyLAN (IEEE 802.12) opracowany został głównie przez firmę Hewlett Packard. Przezwyciężył on problem rywalizacji przez zastosowanie metody opartej na priorytetach, zwanej metodą dostępu z wykorzystaniem priorytetu na żądanie DPAM (*ang. Demand Priority Access Method*). W odróżnieniu od Fast Ethernetu, węzły dołączone są zawsze do huba, który przepatruje regularnie wszystkie porty wejściowe w celu określenia, czy któryś węzeł nie wysyła żądania dostępu.

Standard 100VG-AnyLAN posiada wbudowany mechanizm priorytetów z dwoma poziomami: żądanie o wysokim priorytecie i żądanie o priorytecie normalnym. Żądanie z priorytetem normalnym używane jest do przesyłania danych w czasie nierzeczywistym, takich jak pliki, itp., natomiast żądanie z priorytetem wysokim ma zastosowanie podczas operacji na danych w czasie rzeczywistym, takich jak mowa czy wideo. Obecnie wykorzystanie tych cech jest ograniczone i nie ma mechanizmu wspomagającego te udogodnienia po opuszczeniu przez dane huba.

Sieć 100VG-AnyLAN pozwala na zastosowanie hubów do siedmiu poziomów (to znaczy jeden korzeń i sześć hubów kaskadowych) przy maksymalnej odległości między węzłami równej 150 m.

Migracja do Fast Ethernetu

Jeśli istniejąca sieć oparta jest na standardowym Ethernecie, to w większości przypadków, najlepszym sposobem modernizacji jest przejście na Fast Ethernet lub na sieć 100VG-AnyLAN. Ponieważ protokoły i metody dostępu są takie same, nie potrzeba zmieniać programów zarządzania siecią ani innych aplikacji programowych. Droga migracji do Fast Ethernetu jest prosta i może zawierać:

- unowocześnianie węzłów o dużych szybkościach transmisji, takich jak serwery lub „silne" stacje robocze.
- stopniowa wymiana kart sieciowych NIC (*ang. Network Interface Cards*) w segmentach Ethernetu na karty umożliwiające pracę na dwóch szybkościach transmisji (to znaczy 10 Mb/s i 100 Mb/s).

Droga migracji do sieci 100VG-AnyLAN jest nieco trudniejsza, gdyż sieć ta zależy od hubów i w odróżnieniu od Fast Ethernetu większość kart sieciowych posiada różne złącza sieciowe, jedno dla sieci 10BASE-T a drugie dla sieci 100VG-AnyLAN (możliwe jest również automatyczne rozpoznanie sieci). Droga ta może zawierać:

- unowocześnianie węzłów o dużej szybkościach transmisji, takich jak serwery lub „silne" stacje robocze;
- zainstalowanie hubów 100VG-AnyLAN;

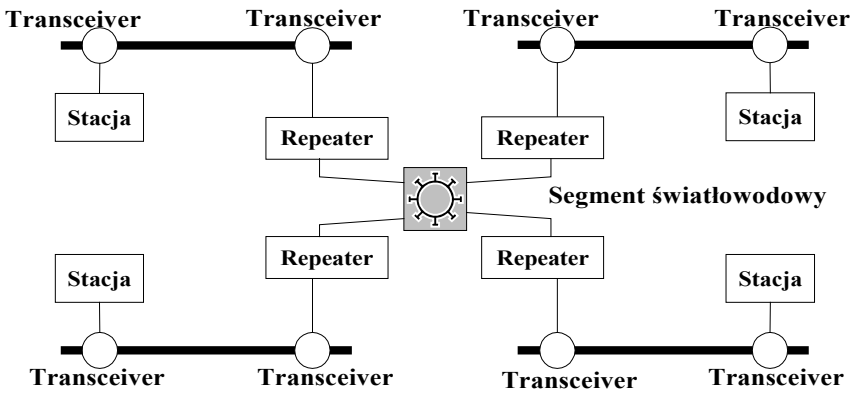
– dołączenie węzłów do hubów 100VG-AnyLAN i zmiana złącz.

Trudno jest ocenić różnice w sprawności działania pomiędzy sieciami Fast Ethernet i 100VG-AnyLAN. Fast Ethernet wykorzystuje sprawdzoną technologię, ale wymaga rywalizacji węzłów o medium. Sieć 100VG-AnyLAN jest relatywnie nową technologią, lecz wymiana informacji z hubem zwiększa czas opóźnienia. Maksymalna przepustowość 100BASE-T ograniczona jest do 50 Mb/s, podczas gdy w przypadku 100VG-AnyLAN jest to wartość 96 Mb/s.

Standard 100BASE-T nie pozwala już na przyszłą modernizację sieci związaną ze zwiększeniem szybkości transmisji danych, podczas gdy standard 100VG-AnyLAN umożliwia na uzyskanie szybkości transmisji do 400 Mb/s.

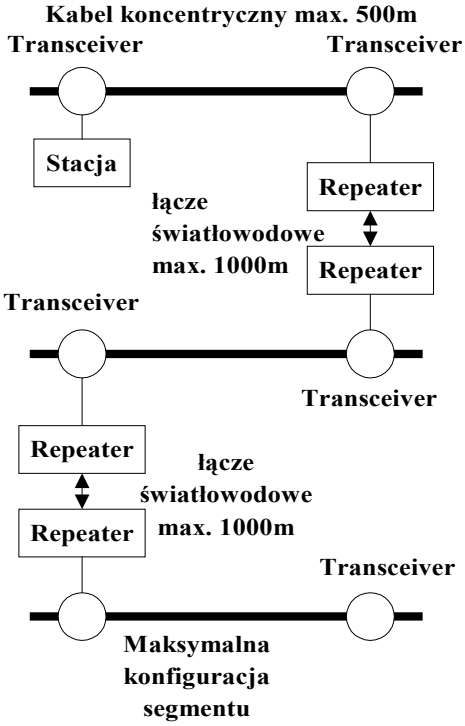
Sieci rozbudowane

Pojedyncze segmenty sieci Ethernet łączone są między sobą za pomocą wzmacniaczy -repeaterów. Są to urządzenia pracujące w warstwie fizycznej modelu odniesieni L&M RM.



Rysunek 3.7 Przykład rozbudowanej sieci Ethernet z wykorzystaniem huba optycznego

Służą zwiększeniu zasięgu transmitowanego sygnału wewnątrz pojedynczej sieci. Urządzenia te nie odgrywają żadnej roli w działaniu protokołu, choć występują także repeatery inteligentne, które eliminują wzajemne oddziaływanie segmentów. Należy zawsze pamiętać o ograniczeniu na długość całkowitą sieci, jaką narzuca długość czasu trwania okna kolizji. W przypadku, gdy chcemy zwiększyć zależności czasowe poza te granice, wtedy (po zwiększeniu okna kolizji) sieć staje się mniej efektywna (zmniejszane jest tym samym efektywnie dostępna przepustowość). Przykłady rozbudowy sieci podano na rysunku 3.7 i 3.8.



Rysunek 3.8 Przykład rozbudowanej sieci Ethernet

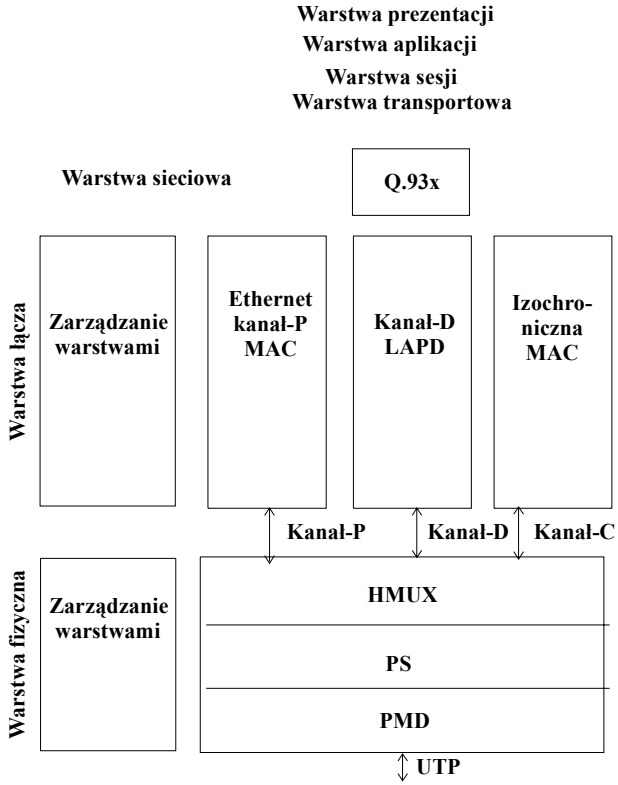
3.2 IsoEthernet

IsoEthernet jest ewolucyjną wersją sieci 10Base-T. Zapewnia on realizacje wymiany danych pakietowych bazując na 10Base-T i trzech liniach pierwotnogrupowych ISDN w pojedynczym styku. Dodatkowo do połączeń bazujących na usługach 10Mb/s Ethernetu (kanał P) zapewniono 96 cyfrowe dupleksowe komutowane kanały 64 kb/s. Kanały zaopatrzone są w te same mechanizmy, które funkcjonują w sieci N-ISDN dla kanałów B. Łączone logicznie kanały B określane są jako kanał C. W celu realizacji procedur w kanale C, takich jak zestawianie i rozłączanie połączeń, utrzymanie i zabezpieczenie w podstawowe i dodatkowe usługi (takie jak połączenia punkt-wielopunkt, połączenia między wieloma punktami jednocześnie, konferencje) wykorzystywany jest oddzielny kanał D o przepustowości 64 kb/s. Jest on, podobnie jak w ISDN, przeznaczony do realizacji procesów sygnalizacyjnych.

Następnym kanałem, który jest definiowany, to kanał M. Jest on kanałem utrzymaniowym, służy do sterowania fizyczną warstwą transportową oraz przekazywania informacji na temat stanu łącza odległego abonenta. Technologia IsoEthernet wykorzystuje dwie pary kabla UTP, co najmniej 3 klasy, którego długość nie może przekroczyć 100 metrów (podobnie zresztą jak dla instalacji Ethernet 10Base-T). Architektura sieci bazuje na konfiguracji gwiazdy, gdzie abonenckie urządzenia końcowe połączone są do centralnego huba/centrali PBX. Specyfikacja IEEE 802.9a definiuje warstwę fizyczną isoEthernetu. Warstwa ta jest najniższą warstwą modelu odniesienia ISO/OSI, a dla sieci lokalnych podzielona została dodatkowo na 3 podwarstwy:

- medium fizycznego PMD (*ang. Physical Medium Dependent*);
- sygnalizacji SP (*ang. Physical Signalling*);

– multipleksacji hybrydowej HMUX (*ang. Hybrid Multiplexing*).



Rysunek 3.9 Architektura modelu specyfikacji IsoEthernet

Rysunek 3.9 przedstawia model warstwowy sieci IsoEthernet na tle modelu siedmiowarstwowego ISO/OSI. Kanał P wykorzystuje warstwę sterowania dostępem do medium MAC tak jak w CSMA/CD, umożliwia to współpracę produktów Ethernetu z warstwą fizyczną IsoEthernetu. Jednocześnie produkty ISDN mogą wykorzystywać fizyczne kanały C i D IsoEthernetu z podwarstwy sterowania dostępu do medium (ITU LAPD, ITU Q.93x).
Warstwa fizyczna zapewnia mechanizmy transportowe dla wszystkich kanałów. Warstwa ta, jak wcześniej sygnalizowano, podzielona jest na podwarstwy:

– HMUX, ze stykiem do kanału: P (Ethernet MAC), kanału C, kanału D MAC. HMUX multipleksuje strumienie danych w jeden strumień, który przesyłany jest do warstwy niższej PS. W kierunku przeciwnym (od strony warstwy fizycznej) podwarstwa odpowiedzialna jest za demultipleksację poszczególnych strumieni informacji.
– PS odbiera strumień informacji w postaci strumienia oktetów z podwarstwy HMUX, zaopatruje ją w wiadomości o multipleksacji TDM, koduje wykorzystując kod 4B/5B (taki jak dla FDDI) i przekazuje do podwarstwy PMD. Realizuje także dekodowanie strumienia informacji odbieranego z przeciwnego kierunku.
– PMD koduje/dekoduje wiadomości w kod wykorzystywany do transmisji w medium NRZI oraz zabezpiecza w styki elektryczne dostępu do medium - dla kabla UTP klasy 3 lub wyższej.

Multipleksacja informacji w sieci IsoEthernet

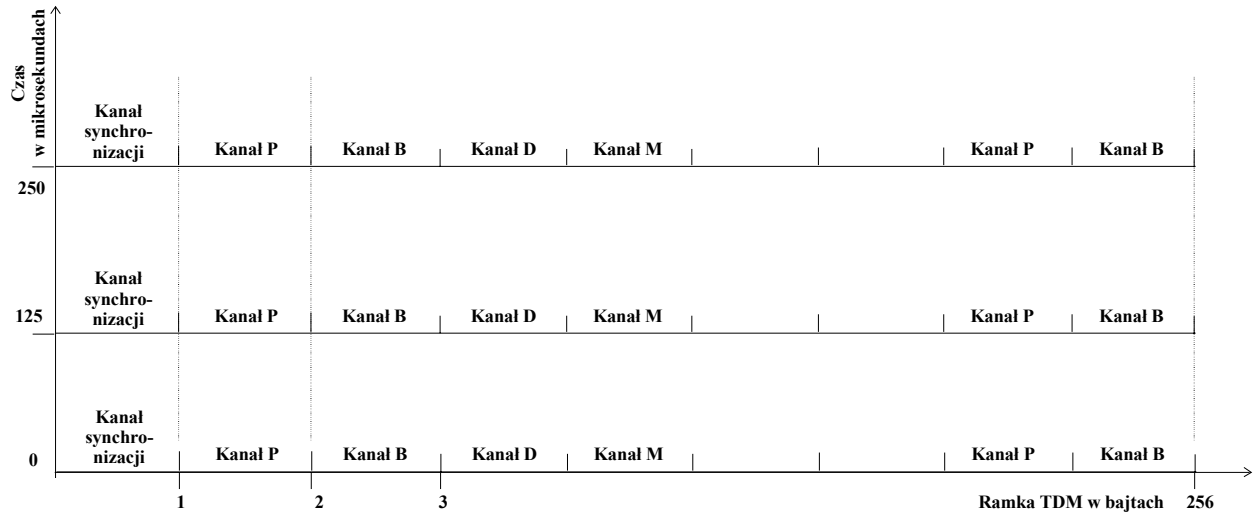
Zabezpieczenie w usługi także te, które są uwarunkowane czasowo, jest możliwe dzięki wykorzystaniu techniki TDM. Strumień informacji przenoszony jest w 125μs

ramkach TDM. Każda ramka zawiera 256 bajtów informacji, odpowiadających multipleksowanym kanałom. W ten sposób gwarantuje ona odpowiednią przepustowość definiowanym wcześniej kanałom P, C, D oraz M.

Podobnie jak ma to miejsce w teletransmisyjnych systemach PCM, ramka zawiera element fazujący (*ang. Start of Frame Delimiter*) umożliwiający rozpoznanie początku ramki a tym samym określenie kolejności poszczególnych kanałów. Zabezpieczają to układy PLL (*ang. Phase Lock Loops*) zastosowane na obu końcach łącza. Synchronizują one ramki a także odzyskują sygnały zegarowe, które są podstawą działania aplikacji multimedialnych - aplikacji czasu rzeczywistego.

Co 125μs ramka TDM wypełniana jest informacjami napływającymi z podwarstwy HMUX. Na rysunku 3.10 przedstawiono sposób jej wykorzystania przez każdy z kanałów.

- kanał P, w zależności od konfiguracji na etapie autonegocjacji procesu sygnalizacji, jest kanałem półdupleksowym albo dupleksowym 10Mb/s, przenoszącym informację pakietową Ethernetu z wykorzystaniem protokołu CSMA/CD MAC;
- kanał C, dupleksowy, wykorzystywany przez usługi wymagające komutacji kanałów, może być (w zależności od konfiguracji) wykorzystywany w jednym z dwóch trybów:
- izochronicznym, obsługuje wtedy kanały wymagające przepustowości od 64 kb/s aż do 15.872 Mb/s;
- wielousługowym, gdzie dostępne jest pasmo 6.144 Mb/s;
- kanał D, dupleksowy o przepustowości 64 kb/s, służy do przekazywania, zabezpieczonych pakietowo, informacji sygnalizacyjnej skojarzonej z kanałem C. Także, analogicznie do rozwiązań ISDN-owskich, w kanale można realizować przesyłanie pakietów wg protokołu X.25;
- kanał M, dupleksowy o przepustowości 96 kb/s, służy do przekazywania informacji utrzymaniowej i synchronizacyjnej (8 kb/s);
- kanał fazowania ramki (*ang. Start of Frame*) - 64 kb/s kanał przenoszący informację na podstawie której rozpoznawany jest początek nowej ramki w szczelinie czasowej T=125μs. W kanale realizowane są także procedury dosynchronizujące układy pętli synchronizacji fazy - PLL do częstotliwości 8 kHz.



Rysunek 3.10 Przykład multipleksacji z podziałem czasu

Tryby pracy IsoEthernetu

Urządzenia sieci IsoEthernet mogą pracować w trzech różnych trybach:

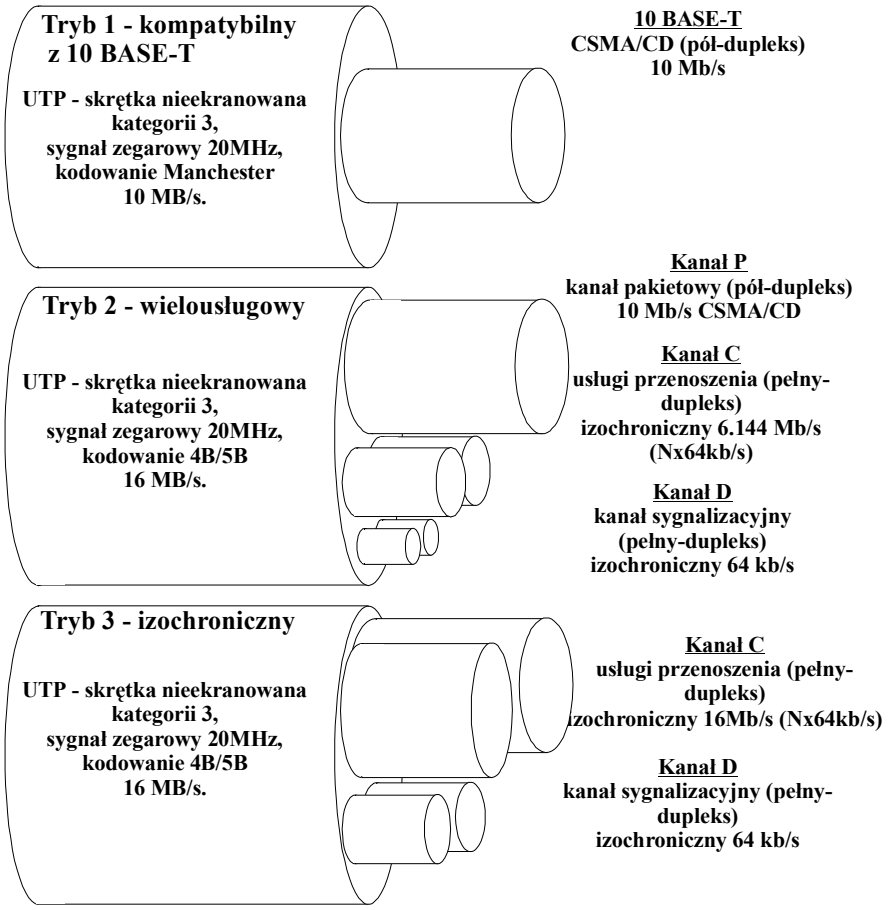
- wielousługowym;
- izochronicznym;
- standardowym 10Base-T.

Tryby są konfigurowane automatycznie po załączeniu zasilania w urządzeniach końcowych sieci, z wykorzystaniem algorytmów sygnalizacyjnych autonegocjacji. W ten sposób zapewniona jest współpraca urządzeń Ethernetu z nowszymi urządzeniami IsoEthernetu w jednej sieci LAN. Nowe Huby isoEthernetu, dzięki algorytmom sygnalizacyjnym autonegocjacji, wykrywają typ urządzenia końcowego i obsługują je zgodnie z opisami standaryzacyjnymi. Jeśli będzie to karta Ethernetu, port huba zostanie automatycznie skonfigurowany do trybu standardowego 10Base-T.

Poszczególne tryby pracy zapewniają realizację następujących usług:

- **tryb wielousługowy**. Zapewniane są usługi takie jak w sieci 10Base-T, jak i usługi komutacji kanałów. Przepustowość łącza podzielona jest w następujący sposób:
  - kanał P o przepustowości 10 Mb/s;
  - kanał C o przepustowości 6.144 Mb/s, który składa się z 96 kanałów typu B (64 kb/s);
  - kanał D (64 kb/s);
  - kanał M (96 kb/s);
  - kanał fazowania ramki (64 kb/s);
- **tryb izochroniczny**, wszystkie usługi realizowane są z wykorzystaniem techniki komutacji kanałów. W trybie tym nie występuje kanał P (w którym realizowany jest protokół CSMA/CD MAC). Strumień wiadomości zabezpieczany jest kodem 4B/5B, a następnie transformowany do formatu NRZI w celu transmisji informacji w medium.
- **tryb 10 Base-T**, warstwa fizyczna IsoEthernetu jest identyczna z 10 Base-T, informacje w linii kodowane są kodem Manchester. Wstępuje tylko kanał P wykorzystujący do transmisji informacji ramki CSMA/CD na podstawie MAC.

Na rysunku 3.11 przedstawiono podział przepustowości w zależności od trybu pracy sieci.

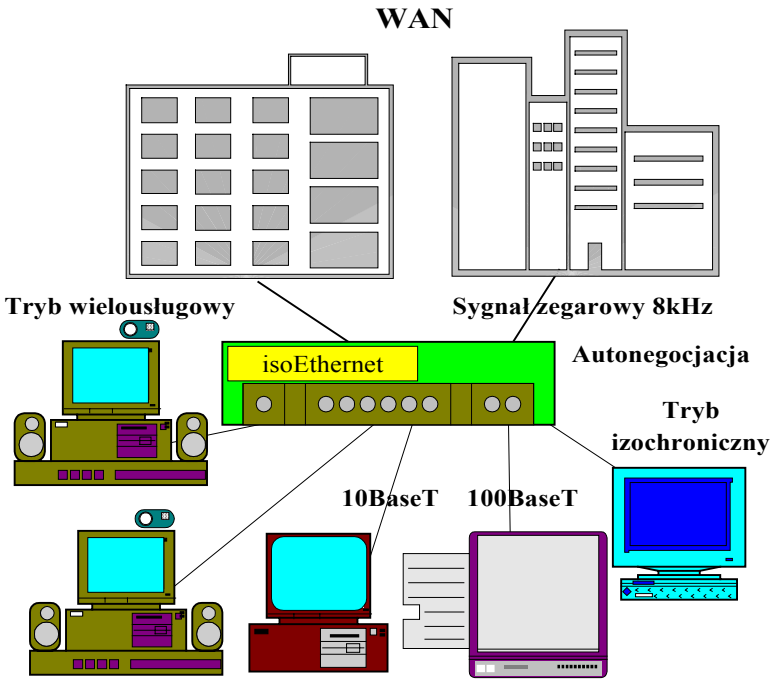


Rysunek 3.11 Podział przepustowości w zależności od trybu pracy sieci IsoEthernet

Algorytm sygnalizacyjny autonegocjacji

Algorytm sygnalizacyjny auto-negocjacji - warstwy fizycznej, umożliwia urządzeniom (w momencie inicjacji pracy) zgłoszenie swoich możliwych trybów pracy. Realizowana jest także rekonfiguracja w celu uzyskania najkorzystniejszych parametrów pracy. W procesie tym wykorzystywane są integralne zmodyfikowane testy 10Base-T, które nie wykorzystują protokołów warstw wyższych. Algorytm umożliwia urządzeniom na obu końcach łącza żądanie i potwierdzanie użytkowania wspólnych trybów pracy pomiędzy dwoma urządzeniami i rezygnacji z tych, które nie są dostępne. W przypadku, gdy możliwych trybów pracy jest kilka, mechanizm umożliwia wybór trybu pracy, którego priorytet jest wyższy i jest zdefiniowany w odpowiedniej, określonej wcześniej tablicy. Algorytm umożliwia, więc przełączanie pomiędzy różnymi trybami pracy w określonych warunkach.

Powyższy schemat zastosowany przez rozwiązania sieci IEEE 802.9a, isoEthernet i IEEE 802.3 (10Base-T, 100BASE-TX), pozwala na łatwą współpracę - interoperacyjność urządzeń. Sieci bazujące na isoEthernecie mogą wykorzystywać/rozpoznawać zdolności systemów 10BASE-T i 100BASE-TX i dynamicznie je przełączać pomiędzy trybami wielousługowym, izochronicznym, 10BASE-T i 100BASE-TX, wykorzystując w algorytmie schemat autonegocjacji. Rysunek 3.12 ilustruje przykład sieci, wewnątrz której różne porty huba isoEthernetu są konfigurowane w celu wykonania operacji zależnych od możliwości urządzeń sieciowych zainstalowanych w PC/stacjach roboczych.



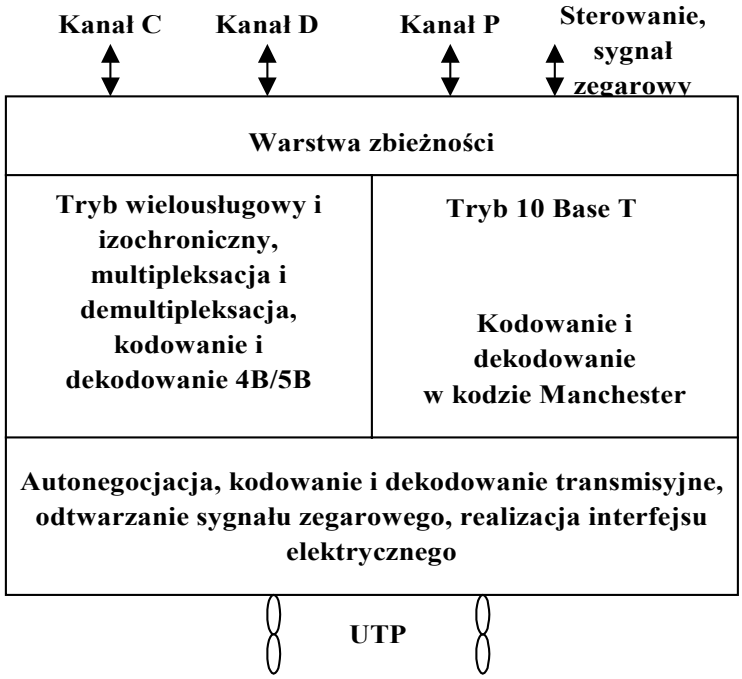
Rysunek 3.12 Przykład topologii sieci IsoEthernet

IsoEthernet umożliwia elastyczny i dynamiczny transfer ramek TDM w segmencie łącza wykorzystującego tryby operacji wielousługowych i izochronicznych. Cecha umożliwia sieci lokalnej isoEthernet współpracę z siecią rozległą WAN, z wykorzystaniem sygnału zegarowego 8 kHz, w kanałach B. Ponadto do sieci isoEthernet można podłączać urządzenia wykorzystujące sygnał zegarowy 8 kHz. Sieć współpracując z urządzeniem może być źródłem bądź odbiorcą sygnałów zegarowych, czyli pracować w trybie Master albo Slave. Przy czym tryb ten ustalany jest automatycznie w procedurach autonegocjacji.

Warstwa fizyczna

W trybach operacji wielousługowej i izochronicznej, warstwa fizyczna isoEthernetu realizuje funkcje multipleksacji kanałów w szczelinach TDM. W celu detekcji błędów, w warstwie łącza danych wykorzystywany jest kod 4B/5B, który przekształcony jest w kod transmisyjny NRZI (*ang. Non Return to Zero Inverted*) a następnie informacja transmitowana jest w medium (UTP). Na odległym końcu dokonywana jest operacja odwrotna, tzn. odbiór wiadomości odbywa się zgodnie z kodem NRZI, który następnie przekształcany jest wg 4B/5B.

W odległej stacji odtwarzane są także sygnały zegarowe oraz demultipleksowane są kanały informacyjne. Na rysunku 3.13 przedstawiona została architektura modelu warstwy fizycznej dla trzech trybów pracy isoEthernetu.



Rysunek 3.13 Model warstwy fizycznej standardu IsoEthernet

Ponieważ algorytm kodowania 4B/5B jest skuteczny i łatwy w implementacji. wykorzystano go w trybie wielousługowym i izochronicznym. Przekształca on czterobitowe sekwencje w zakodowany 5-cio bitowy symbol transmisyjny. Symbole zmniejszają zjawisko powstawania składowej stałej napięcia i minimalizują spektrum częstotliwości w medium transmisyjnym. W czasie transmisji w medium składowa stała mierzona od poziomu nominalnego jest mniejsza niż 10% sygnału. Algorytm kodowania 4B/5B z NRZI zapewnia 80% wykorzystanie przepustowości medium w porównaniu do kodu Manchester (wykorzystywanego w 10BASE-T), który umożliwia tylko 50 % wykorzystanie przepustowości. Zarówno 10BASE-T jak i isoEthernet wykorzystują prędkość sygnałów zegarowych w medium 20MHz, jednak isoEthernet osiąga przepustowość użytkową 16.384 Mb/s zaś 10BASE-T tylko 10 Mb/s.

Jak wcześniej sygnalizowano, stacje końcowe w sieci isoEthernet mogą współpracować z siecią 10BASE-T i wymieniać transparentnie ramki zgodnie z IOS/IEC 8802-3 Ethernet MAC. Zapewnia to możliwość współpracy programów sterowania urządzeniami zgodnych z standardem Ethernet i aplikacji - z siecią isoEthernet - bez żadnych modyfikacji. Aby współpraca sieci 10BASE-T i sieci isoEthernet była możliwa, kanał P wykorzystywany do transportu ramek zgodnych z IOS/IEC 8802-3 Ethernet MAC, musi mieć zaimplementowany identyczny protokół CSMA/CD MAC i musi być umieszczony w tej samej domenie kolizji, co urządzenie sieci 10BASE-T.

Każda ramka transmitowana w kanale P segmentu isoEternet przenosi informacje utajone, które wykorzystywane są przez odległy koniec do utrzymania identycznych parametrów współpracy. Ponadto przenoszona jest w segmencie isoEthernetu informacja o nośnej do odległego końca łącza. W sieciach, w których nie są implementowane procedury powtarzania ramek informacji, ale zapewniają bridging i segmentację sieci, informacje o parametrach sieci Ethernet nie są użytkowane.

W trybie 10BASE-T warstwa fizyczna zachowuje się identycznie jak 10BASE-T z kodem Manchester. Nie jest użytkowane ramkowanie informacji w szczelinach TDM i

zablokowane są usługi kanałów C, D, M. Zapewnia to automatyczną współpracę z urządzeniami sieci 10BASE-T.

Procedury sygnalizacyjne w kanale C

Mechanizmy sygnalizacyjne występujące w sieci isoEthernet są podobne do mechanizmów mających miejsce w sieci ISDN. Realizujący usługi kanał C w zależności od potrzeb może składać się z pewnej liczby kanałów o przepustowości 64 kb/s (kanały B). W celu zabezpieczenia usługom odpowiedniej ich liczby, wykorzystywane są procedury sygnalizacyjne transportujące swe wiadomości w kanale D (rysunek 3.14). Procedury zdefiniowane przez grupę IEEE 802.9a oparte są na rodzinie zaleceń ITU-T Q.93x, które jak wiadomo zostały opracowane dla rozwiązań ISDN, a które obecnie definiowane są dla ATM. Opracowane procedury i protokoły pozwolą na łatwą współpracę pomiędzy sieciami ISDN, ATM i sieciami bazującymi na technologii isoEthernet.

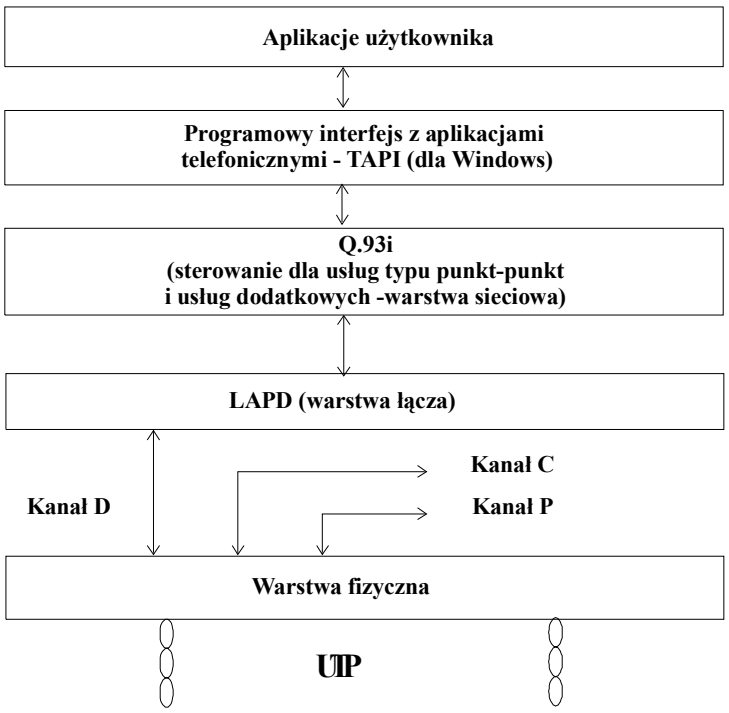
Podstawowe komponenty schematu sygnalizacyjnego można podzielić na:

- Protokół dostępu do łącza w kanale D (LAPD - warstwa 2).
- Procedury współpracy użytkownika z siecią (*ang.User Network Interface*) UNI-IEEE 802.9a Q.93x (Q.931-warstwa 3).
- Procedury współpracy dla usług telefonicznych (ang. Telephony Application Program Interface - TAPI for Windows).

Procedury LAPD - warstwy łącza - są wykorzystywane do enkapsulacji wiadomości Q.93i i ich transportu w kanale D sieci isoEthernet. Pozwalają one na realizację:

- jednego lub kilku połączeń w kanale D;
- wyrównania ramek w warstwie łącza danych;
- sterowania sekwencją ramek w łączu;
- wykrycia transmisji danych w łączu oraz określenie formatu danych w zależności od realizowanego połączenia;
- wykrywania i eliminacji błędów transmisji, formatu danych i operacji w łączu;
- odtwarzania poprawności funkcjonowania protokołów warstwy łącza;
- zarządzania warstwą łącza;
- sterowania przepływem wiadomości.

Procedury sygnalizacyjne Q.93i (w styku użytkownika z siecią) są wykorzystywane do sterowania połączeniami typu punkt-punkt a także do zapewnienia usług dodatkowych (*ang. supplementary services*). Procedury sterowania połączeniami pomiędzy dwoma punktami zapewniają zestawianie, nadzór i zerowanie usług w kanale C. Wiadomości sygnalizacyjne są transportowane pomiędzy określonymi punktami sygnalizacyjnymi urządzeń końcowych oraz hubów isoEthernetu umieszczonymi w warstwach transportowej, sieciowej i łączowej.



Rysunek 3.14 Procedury sygnalizacyjne w sieci IsoEthernet

Wiadomości wykorzystywane w procesie sterowania połączeniami w przypadku realizacji usług podstawowych zostały przedstawione w tabeli 3.3 zaś wiadomości wykorzystywane w celu zapewnienia usług dodatkowych zamieszczono w tabeli 3.4.

Tabela 3.3 Wiadomości Q.93i wykorzystywane w procesie sterowania połączeniami w przypadku realizacji usług podstawowych

Wiadomości zestawiania połączeń	Wiadomości zerowania połączeń
Alerting	Disconnect
Call Proceeding	Release
Connect	Release Complete
Connect Acknowledge	Inne wiadomości
Progress	Status
Setup	Status Inquiry
Setup Acknowledge (opcjonalnie)	Information (opcjonalnie)
Wiadomości odnoszące się do wywołań globalnych	
Restart	Restart Acknowledge

Tabela 3.4 Wiadomości Q.93i wykorzystywane w procesie sterowania połączeniami w przypadku realizacji usług dodatkowych (opcjonalne)

Wiadomości dla podstawowych usług uzupełniających		
Hold	Retrieve	Key Setup
Hold Acknowledge	Retrieve Acknowledge	Key Setup Ack.
Hold Reject	Retrieve Reject	Key Hold
Key Release	Notify	
Wiadomości wykorzystywane w proc. sterowania połączeniami rozsiewczymi		
Add Party	Add Party Ack.	Add Party Reject
Drop Party	Drop Party Ack.	

Usługi dodatkowe zapewniają użytkownikom sieci isoEthernet realizację:

- transferu wywołań - wiadomości o wywołaniu, inicjowanym w kanale C, transferowane są do innych urządzeń końcowych isoEthernetu lub ISDN;
- podtrzymywanie wywołań - wiadomości o wywołaniu, inicjowanym w kanale C, mogą być opóźniane i ponawiane w późniejszym czasie. Funkcja zapewnia realizację aplikacji wielo-usługowych korzystających z tego samego połączenia w kanale fizycznym C;
- konferencyjnych - użytkownicy podłączeni do sieci isoEthernet czy też abonenci sieci ISDN mogą komunikować się ze sobą i uruchamiać sesje konferencyjne korzystając z urządzenia sterowania połączeniami wielopunktowymi - MCU (*ang. Multipoint Control Unit*);
- połączenia punkt-wielopunkt i wielopunkt - wielopunkt - w środowisku sieci lokalnej lub miejskiej, szczególnie ważna jest możliwość zestawiania połączeń pomiędzy jednym źródłem informacji i wieloma jej ujściami oraz między wieloma źródłami/ujściami informacji jednocześnie. Aplikacje, które korzystają z tego typu połączeń, to poczta wideo i audio-foniczna. Środowisko sieci isoEthernet umożliwia realizację jednoczesnej komunikacji wielu użytkowników ze sobą, zapewniając tym samym usługę wideokonferencji. Implementacja tej usługi w sieci isoEthernet charakteryzuje się niskimi nakładami finansowymi, nie wymaga stosowania urządzeń MCU a ponadto zapewnia uczestnikom wideokonferencji możliwość zobrazowania ich na wszystkich monitorach biorących udział w sesji wideokonferencyjnej.

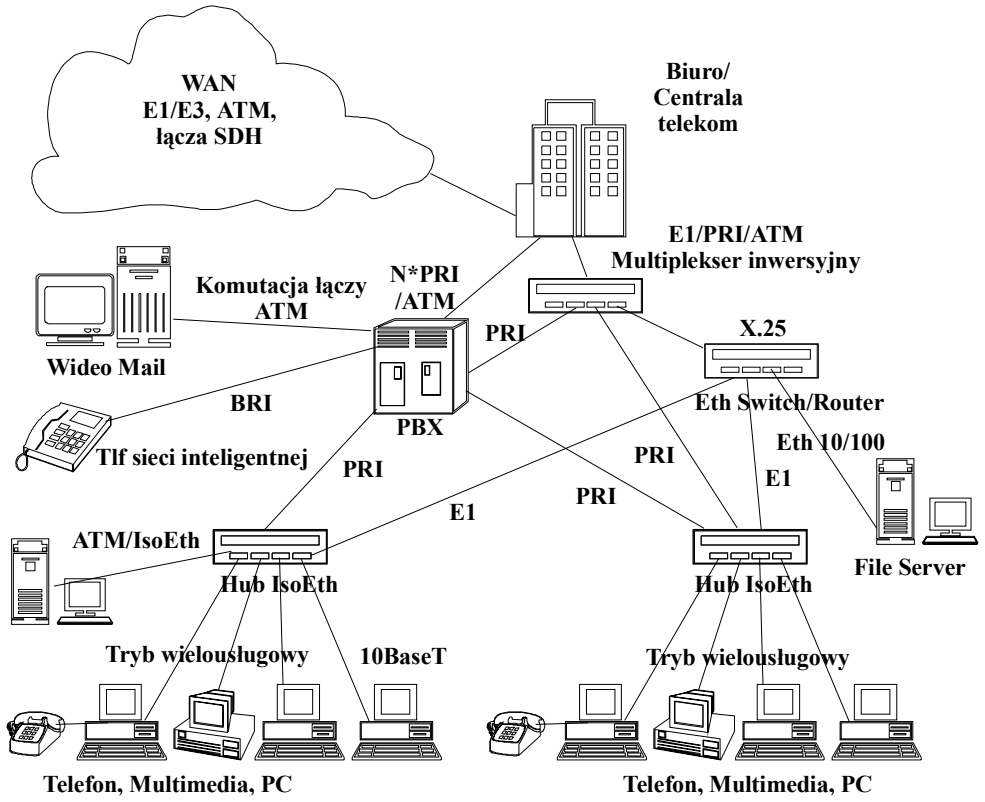
Programowy interfejs aplikacji telefonicznych (TAPI) dla Microsoft Windows jest zaprojektowany podobnie do interfejsu aplikacji użytkownika, który jest stosowany w ISDN. Dzięki temu zapewniona jest współpraca urządzeń abonenckich sieci isoEthernet i sieci ISDN. Interfejs zbudowano tak, by przesłonić technologię transportu informacji, dzięki czemu stworzono komfortowe warunki dla dynamicznego rozwoju nowych aplikacji multimedialnych. Wykorzystywane aplikacje ustawiają odpowiednio parametry interfejsu TAPI, który następnie wpływa na wywołania realizowane w sieci, tak, aby osiągnąć zadowalającą jakość realizowanej usługi (*ang. Quality of Service*).

Topologia sieci

IsoEthernet, podobnie do 10BASE-T, jest siecią o konfiguracji gwiazdy, gdzie urządzenia użytkowników podłączone są do urządzeń sieciowych Hubów/PBX. Jak wcześniej zaznaczono, isoEthernet jest rozwiązaniem sieci lokalnej na bazie, której realizowane są usługi, które w innych sieciach były ze sobą nie do pogodzenia. Sieć zapewnia realizację usług zarówno izochronicznych jak i pakietowych, ponadto może bezpośrednio współpracować z innymi standardowymi sieciami. Obecnie prowadzone są prace nad realizacją w sieci isoEthernet usług w trybie przesyłania komórek (*ang. cell - mode bearer services*). Rysunek 3.15 przedstawia przykład topologii sieci rozproszonej isoEthernet wykorzystywanej przez dużą firmę, która posiada swe oddziały w innych miejscowościach. Do segmentów sieci isoEthernet podłączone są komputery osobiste, stacje robocze, ale także komputery multimedialne. Komunikacja pomiędzy filiami firmy odbywa się z wykorzystaniem zasobów sieci rozległej.

Aplikacje multimedialne uruchamiane w stacjach końcowych mogą współpracować zarówno z aplikacjami sieci wewnętrznej isoEthernet jak i aplikacjami urządzeń końcowych, które są geograficznie oddalone i znajdują się w filiach firmy. Podstawowe usługi audio, zapewnione są w sieci isoEthernet z wykorzystaniem jednego z 64 kb/s kanałów B. Równocześnie z obsługą komputerów multimedialnych, huby isoEthernetu

zapewniają pracę stacjom końcowym podłączonym w trybie 10BASE-T. W przykładowej konfiguracji do segmentów sieci pracujących w trybie izochronicznym podłączone są serwery wideo z aplikacjami wymagającymi dużych szybkości transmisji. Mogą one realizować usługi np. w trybie asynchronicznego transferu. Warstwa transportu informacji gwarantuje odpowiedni poziom jakości usług (QoS). Wymagania dotyczące sygnalizacji w sieciach isoEthernet, ATM i ISDN są podobne, ponadto isoEthernet zapewnia możliwość jednoczesnej pracy w trybach komutacji kanałów, przesyłania komórek jak i przesyłania pakietów.



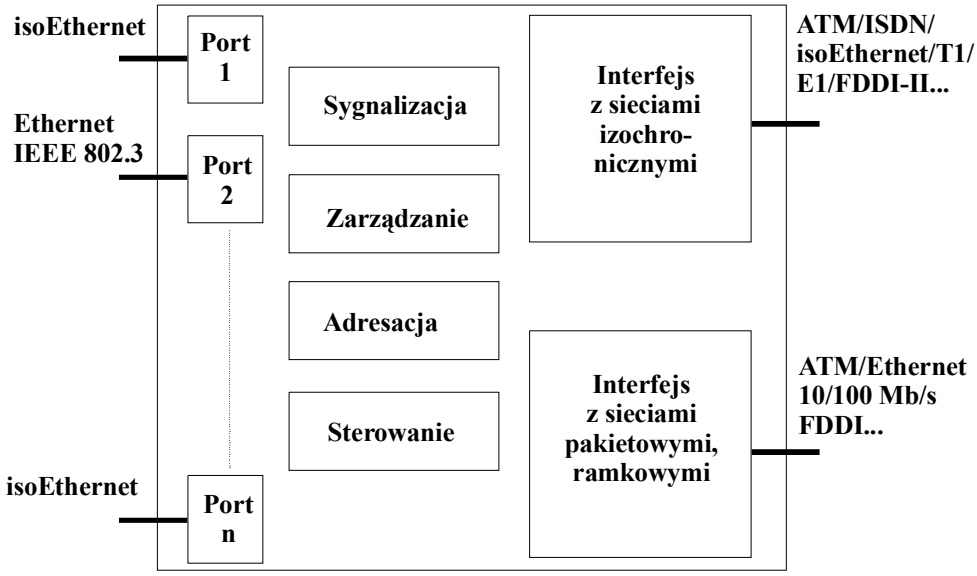
Rysunek 3.15 Przykład topologii sieci rozproszonej isoEthernet wykorzystywanej przez dużą firmę

Jak już wspomniano, omawiany przykład ilustruje rozproszoną architekturę dużej firmy, stąd też rozproszone są także zasoby sieci isoEthernet. Jednak funkcjonalność sieci nie ogranicza się tylko do powyższego przypadku. Dla małych środowisk wymagających sieci lokalnej np. filia firmy albo nieduże biuro konstrukcyjne, proponowany jest inny scentralizowany wariant. Wszyscy użytkownicy podłączani są do jednego huba, który podłączony jest do sieci rozległej. Podobnie jak poprzednio zapewniona jest możliwość realizacji wymiany wszystkich rodzajów informacji tzn. wideo, audio i pakietowych.

Ponieważ obecnie eksploatowane rozległe sieci transmisji danych i mowy różnią się zasadniczo sposobem realizacji przekazu informacji, dlatego sieć multimedialna korzysta z sieci rozległej na zasadzie sieci tranzytowej. Z tego też powodu w przykładzie dla dużej firmy sieć posiada wiele rozproszonych w niej urządzeń sieciowych hubów/PBX do współpracy ze światem zewnętrznym. Zakres funkcji urządzeń dostępowych (hubów i PBX) opisany został w dokumencie *ang. „Functional Specification for AU to AU Internetworking”* przez IEEE 802.9b, projekt D4.2,

wydanym 1 lipca 1994r. Rysunek 3.16 przedstawia podstawowe funkcje, które są realizowane w tych urządzeniach.

Hub/PBX zapewnia łączność pomiędzy wieloma urządzeniami isoEthernetu i/lub urządzeniami 10BASE-T. Przenosi informacje w postaci ramek Ethernetu, a także realizuje komutację i multipleksację pakietów. Hub realizuje funkcje repeatera ramek do/z różnych portów tworzących wspólną domenę kolizji. W zależności od potrzeb hub może realizować funkcje bridgingu i funkcje komutacji ramek w sieci. Może także zapewnić interfejs z podkładowymi sieciami pakietowymi - ATM, FDDI czy też 100Mb/s Ethernetem.



Rysunek 3.16 Model urządzenia dostępowego sieci IsoEthernet

Urządzenie dostępowe zawiera interfejs komutacji i multipleksacji izochronicznej, zapewniający (pomiędzy każdymi jego portami) dynamiczną komutację kanałów C. Styk ten może być wykorzystany do współpracy z innymi sieciami izochronicznymi (ISDN, E1/T1, FDDI-II) czy też sieciami zapewniającymi usługi ze stałą szybkością bitową CBR (*ang. Constant Bit Rate*) np. ATM. AU realizując wcześniej opisane funkcje odpowiada także za procesy zarządzania i sygnalizacji a także adresacje w sieci. Wiadomości sygnalizacyjne są przesyłane i wykorzystywane w celu dynamicznej komutacji kanałów C wewnątrz jak i pomiędzy urządzeniami. Dołączone do urządzenia dostępowego stacje końcowe oraz integralne porty samego AU są zarządzane i sterowane poprzez funkcje zarządzające. Procedury adresacji odpowiadają za właściwą marszrutyzację informacji w sieci.

ATM - isoEthernet

ATM jest technologią opartą na przesyłaniu komórek o stałym 53 oktetowym rozmiarze wewnątrz zestawionych połączeń wirtualnych. Warstwa fizyczna oparta jest o synchroniczne systemy teletransmisyjne, stąd też rozwiązanie to jest technologią skalowalną. Warstwa adaptacyjna ATM (*ang. ATM Adaptation Layer 1÷5*) zapewnia obsługę ruchu połączeniowego jak i bezpołączeniowego oraz współpracuje z aplikacjami o stałej i zmiennej szybkości bitowej. Istnieje możliwość współpracy pomiędzy ATM i isoEthernetem. Obydwa rozwiązania wykorzystują protokoły sygnalizacyjne, służące do zestawiania połączeń, bazujące na zaleceniu Q.93x.

Mechanizmy realizacji połączeń rozsiewczych także są podobne. Powyższe cechy umożliwiają łatwą współpracę pomiędzy sieciami isoEthernet i ATM. Warstwa fizyczna ATM obsługuje warstwy AAL od 1 do 5 i ruch generowany w tym interfejsie. Dla aplikacji transmisji mowy jest wymagany interfejs izochroniczny, który jest dzielony pomiędzy usługi ze stałą i zmienną szybkością bitową. IsoEthernet pracujący w trybie izochronicznym czy też wielousługowym zapewnia odpowiednią funkcjonalność na bardzo niskim poziomie kosztów, ponadto może być wykorzystane jako tanie rozwiązanie współpracujące z urządzeniami końcowymi ATM. Komórki ATM mogą być w bardzo łatwy sposób przenoszone w kanale C, który jest dynamicznie konfigurowalny zgodnie z żądaniami generowanymi przez źródła ruchu ATM. W związku z tym, jeśli występuje taka potrzeba, sieć isoEthernet może być wykorzystywana do współpracy z urządzeniami końcowymi ATM.

W związku z możliwością komutacji i multipleksacji izochronicznej, AU może skonfigurować swe izochroniczne kanały C tak, by stać się pomostem teletransmisyjnym dla komórek przesłanych w sieci podkładowej ATM. Zatem isoEthernet jest bardzo elastycznym rozwiązaniem w zmieniającym się środowisku sieciowym. Jest nie tylko kompatybilny z istniejącymi cyfrowymi sieciami rozległymi, ale także z rozwijającą się technologią ATM. Jednocześnie w środowisku sieci lokalnych jest kompatybilny ze swym przodkiem 10BASE-T (która niepodzielnie dominuje w sektorze sieci lokalnych), ale może także współpracować z CSMA/CD 100Mb/s (100BASE-TX/T4).

Aplikacje multimedialne w isoEthernecie

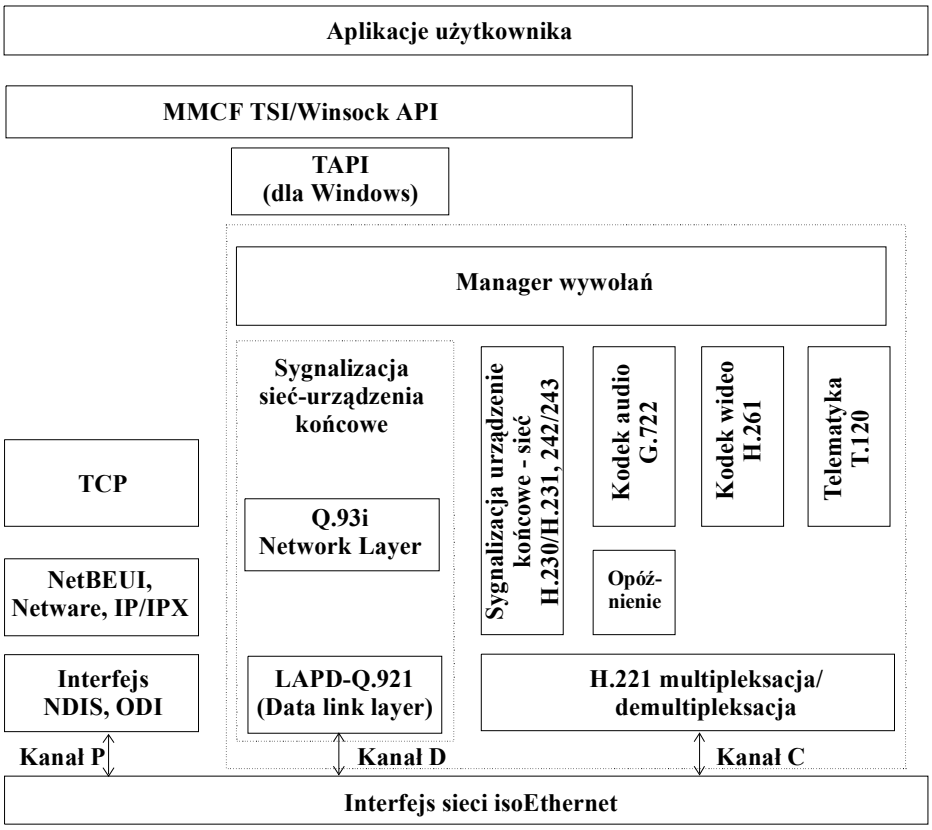
Idea komunikacji multimedialnej MMDC (*ang. Multimedia Desktop Collaboration*) oparta jest na kombinacji konferencji wideofonicznej i jednoczesnej współpracy procesów przetwarzania informacji, przebiegających w komputerach i między nimi. Prowadzona komunikacja pomiędzy abonentami jest na tyle efektywna, na ile pozwala aplikacja czasu rzeczywistego obejmująca jej użytkowników.

Grupa robocza 15 ITU-T zdefiniowała w roku 1990 zalecenia H.320 (*ang. Narrowband Visual Telephony Systems and Terminal Equipment*) i w roku 1995 H.322 (*ang. Visual Telephony Systems and Terminal Equipment for Local Area Networks which provide a Guaranteed Quality of Service*). Stały się one dominującymi standardami dla tworzonych aplikacji MMDC. Zalecenie H.320 było przeznaczone oryginalnie dla usług sieci wąskopasmowej ISDN. Później zostało zmodyfikowane dla sieci lokalnych (H.322), które zapewniają identyczną jakość usług jak sieć N-ISDN. Rysunek 3.17 ilustruje aplikacje MMDC wg H.322, która występuje w sieci isoEthernet. H.322 zapewnia transport skompresowanych strumieni informacji realizowanych usług audio i wideo, które są multipleksowane/demultipleksowane przez warstwę niższą opisaną zaleceniem H.221. Kodeki mowy wykorzystują algorytmy ITU-T G.711/G.722/G.728 zaś kompresja wideo realizowana jest zgodnie z algorytmem H.261.

Obsługa sygnalizacji dokonywana jest w paśmie przesyłania informacji użytkowej zgodnie z H.230/231 i H.242/243. Obsługa transmisji pakietów wewnątrz kanału transmisyjnego (realizującego usługi wg H.322) realizowana jest zgodnie z protokołem T.120. Protokół ten zapewnia transfer plików, przesyłanie komunikatów, informacji sterujących konferencją itd. Zestawianie i rozłączanie połączeń oraz usługi dodatkowe dostępne są z warstwy TAPI, komunikującej się z procedurami Q.93i i Q.921 za pomocą zarządcy wywołań (*ang. Call Manager*). Obsługa protokołów pakietowych

TCP, wykorzystywanych przez sieci bazujące na IP/IPX, realizowana jest identycznie jak w sieci Ethernet. IsoEthernet transportuje pakiety w kanale P.

Interfejsy dla usług transportowych (*ang. Transport Services Interface Multimedia Communication Function*) TSI MMCF/Winsock API zapewniane są przez warstwę usytuowaną pomiędzy aplikacjami użytkownika i protokołami niższych warstw. Interfejs realizuje usługę transportu na rzecz wielu aplikacji, których poziom jakości usług może być różny. Do określenia poziomu jakości zobligowane są aplikacje użytkownika na etapie fazy zestawiania połączenia. Warto zauważyć, że interfejs z warstwami niższymi jest tak skonstruowany, by aplikacje użytkownika nie musiały „wiedzieć", jaka technologia transportu informacji jest wykorzystywana.



Rysunek 3.17 Architektura aplikacji MMDC H.322 w IsoEthernet

Standaryzacja isoEthernetu

Prace nad wykorzystaniem i rozwijaniem techniki isoEthernetu prowadzi komitet standaryzacyjny ISLAN IEEE 802.9. Szczególny nacisk położony jest na rozwój standardów:

- IEEE 802.9b (współpraca pomiędzy urządzeniami AU);
- IEEE 802.9e (tryb obsługi ATM);
- IEEE 802.9f (zdalne zasilanie urządzeń abonenckich).

IEEE 802.9b definiuje funkcjonalność urządzeń dostępowych sieci isoEthernet. W szczególności określa możliwości współpracy i operacje AU dostępne lokalnie i dostępne z wykorzystaniem sieci rozległej. Ta część standardu jest istotna dla użytkowników, którzy są oddaleni od siebie geograficznie. Dzięki IEEE 802.9b użytkownicy mogą pracować między sobą, tak jakby znajdowali się w tej samej sieci lokalnej. Cecha ta zapewnia skalowalność technologii isoEthernet.

IEEE 802.9e definiuje współpracę sieci isoEthernet z siecią ATM. Jest to możliwe dzięki wprowadzeniu do sieci isoEthernet trybu transferu asynchronicznego.

IEEE 802.9f określa sposób zasilania urządzeń końcowych z wykorzystaniem okablowania służącego jednocześnie do transmisji informacji. Zapewni to realizację usługi transmisji mowy z urządzeń nie posiadających lokalnych źródeł zasilania.

Komitet standaryzacyjny IEEE 802.9 przy współpracy z jednostkami przemysłowymi zapewni efektywny proces rozwoju technologii multimedialnej i wprowadzania jej szeroko na rynek teleinformatyczny. Czuwa nad zdolnością współpracy isoEthernetu z istniejącymi oraz przyszłymi sieciami lokalnymi i rozległymi.

3.3 Sieci pierścieniowe

Rodzaje sieci pierścieniowych

W sieciach o topologii pierścienia stosuje się trzy główne metody sterowania dostępem do medium transmisyjnego (a zarazem - typy warstwy MAC), z którymi często identyfikowany jest rodzaj sieci:

- pierścień z przesyłaniem znacznika (*ang. token ring*);
- pierścień szczelinowy (*ang. slotted ring)*;
- pierścień z wtrącanym rejestrem (*ang. register insertion ring*).

Mimo, że metoda przesyłania znacznika stosowana jest również w sieciach o topologii szyny (*ang. token bus*), wszystkie wymienione metody dostępu korzystają w sposób istotny z cech topologii pierścieniowej. Generalna zasada pracy wszelkich sieci pierścieniowych daje się sprowadzić do następujących punktów:

- stacja mająca do nadania ramki uzyskuje chwilowy dostęp do medium na podstawie obserwacji jego aktywności, zgodnie z określoną procedurą;
- kolejne stacje retransmitują odebrany od poprzednika sygnał cyfrowy, wprowadzając przy tym określone opóźnienie (wyrażone w ilości bitów);
- stacja przeznaczenia (zaadresowana przez nadawcę) odbiera (kopiuje) ramkę;
- nadana ramka jest następnie (po spełnieniu swej roli) usuwana z pierścienia.

Zadania i procedura wyboru stacji - monitora

Podstawowy protokół dostępu do medium w sieciach pierścieniowych jest symetryczny (identyczny "program" w każdej ze stacji). Jednakże zwykle stosuje się wydzieloną stację- monitor (określony na stałe lub wybierany dynamicznie spośród wszystkich stacji pierścienia), która spełnia jedną (lub więcej) z następujących funkcji:

- wymuszanie taktu zegarów transmisyjnych (szybkość transmisji w medium);
- zbieranie i reagowanie na ramki służbowe (awaryjne);
- inicjalizacja pracy pierścienia;
- wspomaganie realizacji transmisji do wszystkich odbiorców (*ang. broadcast*);
- nadzorowanie jakości transmisji i reagowanie na ramki zniekształcone.

Dynamicznego wyboru stacji-monitora dokonuje się z reguły na zasadzie rywalizacji adresów, np. w sposób opisany poniżej:

- Każdej stacji przyporządkowuje się unikalny adres sieciowy.
- Po rozpoczęciu procedury wyboru, każda stacja A przesyła do stacji kolejnej B ramkę służbową, zawierającą własny adres A.
- Stacja B, odbierająca taką ramkę, retransmituje ją do stacji kolejnej C tylko wtedy, gdy A>B (gdy adres odebrany jest wyższy od adresu własnego). W przeciwnym wypadku ramka nie jest retransmitowana dalej.
- Stacja, która odbierze ze stacji poprzedniej ramkę, zawierającą własny adres, przejmuje rolę stacji-monitora. Jest to stacja o adresie najwyższym spośród adresów wszystkich stacji sieci (kolejne stacje przekazały jej ramkę dookoła pierścienia zaś ramki innych stacji zostały po drodze "zjedzone").

Usuwanie ramki

Istnieją trzy sposoby usuwania (fizycznego bądź jedynie logicznego) ramki z pierścienia:

- usuwanie przez stację zaadresowaną (*ang. destination removal*);

- usuwanie przez stację nadającą, po obiegnięciu ramki wokół pierścienia (*ang. source removal*);
- usuwanie przez stację-monitor (dotyczy z reguły ramek przekłamanych lub typu broadcast).

Sposoby te mogą dotyczyć wszelkich metod dostępu do pierścienia (rozumianych jako zasady wprowadzania własnej ramki) - są od nich w zasadzie niezależne. Należy jednak zauważyć, że w praktyce danemu typowi MAC przyporządkowuje się "najwłaściwszy" dla niego sposób usuwania ramek:

- destination removal dla register insertion;
- source removal dla slotted ring i token ring.

Przesyłanie ramki do wszystkich stacji

Wykorzystanie wspólnego, dzielonego medium transmisyjnego o topologii pierścienia (podobnie jak w przypadku szyny) pozwala na realizację dwóch podstawowych usług jako pojedynczej operacji:

- przesłanie ramki do określonej stacji, opisywanej przez jej indywidualny, unikalny adres;
- przesłanie ramki do wszystkich stacji (broadcast), w wyniku użycia specjalnego adresu, rozpoznawanego jako "swój" przez każdą ze stacji.

Przy zastosowaniu source removal usługę typu broadcast realizuje się w naturalny sposób - każda ramka obiega (w wyniku retransmisji przez kolejne stacje) cały pierścień, a zatem może być skopiowana przez każdą ze stacji.

Przy destination removal ramka z zasady obiega tylko część pierścienia (między stacją nadającą a odbierającą). Do realizacji usługi broadcast stosuje się wtedy pewne modyfikacje protokołu, z użyciem wyróżnionej stacji-monitora.

Poniżej omówiono trzy generyczne typy protokołów warstwy MAC dla sieci o topologii pierścienia.

Token ring - pierścień z przesyłaniem znacznika

Uwaga. Warstwa MAC dla pierścienia z przesyłaniem znacznika jest przedmiotem dokumentu IEEE 802.5. Jest to dość skomplikowany protokół, bardzo zbliżony do zastosowanego przez firmę IBM w znanej sieci IBM Token Ring. Istnieją znacznie prostsze realizacje.

Zasada działania

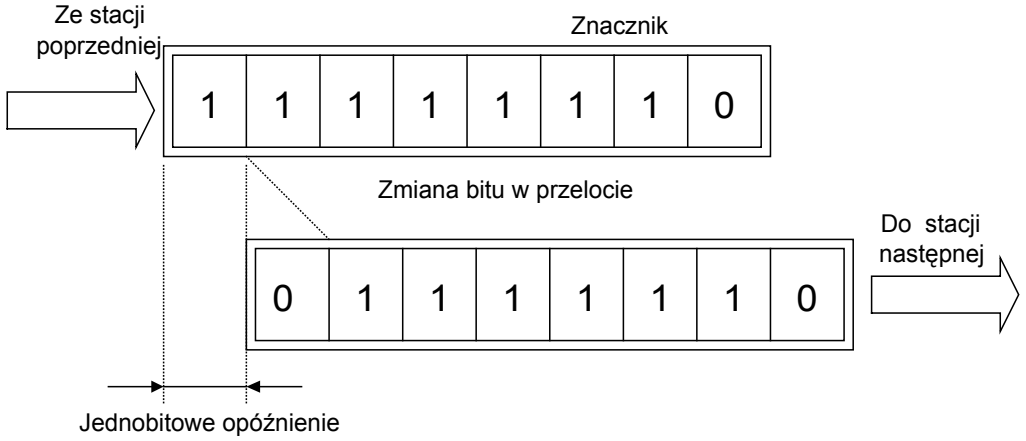
- W pierścieniu krąży (jest kolejno retransmitowany) jeden i tylko jeden unikalny (nie do "podrobienia" przez ciąg danych) ciąg służbowy zwany znacznikiem (*ang. token*). Odebranie znacznika przez stację jest równoznaczne z uzyskaniem przez tą stację prawa do nadawania.
- Po odebraniu znacznika stacja pragnąca nadawać, usuwa znacznik z sieci a następnie wprowadza (nadaje) własną ramkę.
- Po usunięciu znacznika żadna inna stacja nie na możliwości nadania własnej ramki (brak znacznika w sieci).
- Po wykorzystaniu nadana ramka musi zostać usunięta z pierścienia (zgodnie z przyjętą zasadą usuwania).

Uwaga: przyjęło się uważać usuwanie ramki przez stację nadającą (*ang. source removal*) za sposób właściwy dla sieci typu token-ring.

Po nadaniu ramki, do sieci musi zostać ponownie wprowadzony znacznik, aby umożliwić nadawanie przez kolejne stacje.

W celu maksymalnego wykorzystania medium dąży się do minimalizacji opóźnienia retransmisji w każdej ze stacji. Zwykle opóźnienie to wynosi zaledwie 1 bit i jest stałe.

W związku z tym, usuwanie znacznika (na początku nadawania) musi dokonywać się "w biegu" (podczas retransmisji), np. w następujący sposób (rysunek 3.18).



Rysunek 3.18 Zmiana znacznika z wolnego na zajęty

- postać znacznika różni się od postaci ciągu "pustego", nie będącego znacznikiem (a pełniącego rolę np. ciągu początkowego - headera ramki) wartością tylko jednego bitu, przy czym jest to bit ostatni w sekwencji znacznika;
- stacja pragnąca nadawać rozpoznaje znacznik; w chwili jego rozpoznania wszystkie bity znacznika, z wyjątkiem ostatniego, zostały już retransmitowane do stacji kolejnej (opóźnienie w stacji - tylko 1 bit);
- zamiast retransmitować ostatni bit znacznika, stacja zmienia jego wartość "w przelocie", dzięki czemu stacja kolejna odbiera sekwencję początkową ramki (nie będącą znacznikiem);
- z chwilą zamiany znacznika w sekwencję początkową, stacja przełącza się w stan nadawania: zaprzestaje retransmisji bitów ze stacji poprzedniej (odłącza logicznie własny nadajnik od własnego odbiornika) i rozpoczyna nadawanie dalszego ciągu własnej ramki (jej początek został już nadany).

W związku z takim sposobem usuwania znacznika stosuje się często następującą terminologię:

- znacznik wolny (*ang. free token*) - prawo do nadawania;
- znacznik zajęty (*ang. busy token*) - początek ramki, uzyskany w wyniku celowego przekłamania znacznika wolnego.

Postać znacznika

Unikalną postać znacznika można uzyskać na jeden z następujących sposobów:

- stosując bit stuffing, wzorowany na protokole HDLC (token: 01111111, flag: O1111110, ciąg danych: po każdych pięciu bitach 1 wtrącane jest zero) znaczną część protokołu dostępu do medium można wtedy zrealizować w prosty sposób z użyciem popularnych układów scalonych do transmisji synchronicznej, nawet tak prostych, jak np. Z80 SIO;

- stosując zaburzenia kodu transmisyjnego (np. *ang. differential Manchester* - elementy zaburzone, nie występujące w ciągu danych) jest to rozwiązanie stosowane w sieci IBM Token Ring;
- wykorzystując dwa oddzielne pierścienie fizyczne: w jednym krąży wyłącznie impuls, pełniący rolę znacznika, w drugim - prowadzi się transmisję ramek użytkowych (znane, lecz nieekonomiczne i bardzo rzadko stosowane rozwiązanie).

Strategia wprowadzania znacznika

Stosowane są trzy strategie wprowadzania nowego znacznika (wolnego) przez stację, która uprzednio usunęła znacznik (nadała własną ramkę):

- single frame;
- single token;
- multiple token.

Na wstępie należy przypomnieć, że w trakcie nadawania stacja odbiera bity ze stacji poprzedniej, lecz ich nie retransmituje. Zauważmy, że przy source removal (w warunkach poprawnej pracy sieci) pierwszą ramkę, którą stacja nadająca odbierze ze stacji poprzedniej, będzie ramka własna (nadana przez tę właśnie stację) - jest to niezmiennik sieci token-ring.

Przy zastosowaniu strategii single frame, stacja nadająca oczekuje na odebranie końca własnej ramki (po obiegnięciu pierścienia przez tę ramkę), a następnie wprowadza (nadaje) wolny znacznik. Wprowadzenie nowego znacznika może wtedy nastąpić natychmiast, gdyż fakt odebrania końca ramki implikuje wcześniejsze zakończenie nadawania tej ramki. Po nadaniu znacznika stacja przełącza się natychmiast w stan retransmisji. Omawiana tu strategia dobrze nadaje się do zastosowania w sieci, w której długość ramki jest (znacznie) większa od "długości bitowej" pierścienia, czyli gdy czas bezproduktywnego oczekiwania na obiegnięcie pierścienia przez koniec ramki może być zaniedbany w stosunku do całkowitego czasu transmisji ramki. Jest to również strategia najmniej złożona i najbardziej "bezpieczna".

W strategii single token stacja nadająca oczekuje na odebranie początku nadanej przez siebie ramki, zawierającej znacznik zajęty i (zwykle) adres ramki. Po odebraniu początku ramki stacja wprowadza nowy znacznik, lecz przełącza się w stan retransmisji dopiero po odebraniu końca ramki (w ten sposób ramka jest usuwana z pierścienia). Zauważmy, że nadanie znacznika może nastąpić dopiero po zakończeniu nadawania własnej ramki. Dlatego omawiana strategia może być stosowana, jeśli długość ramki jest mała w porównaniu z "długością bitową" pierścienia, czyli gdy odebranie początku ramki oznacza zarazem, że koniec tej ramki został już nadany. Nazwa single token odnosi się do faktu przebywania w pierścieniu tylko jednego znacznika (wolnego lub zajętego), co ułatwia kontrolę poprawności pracy sieci.

W strategii multiple token, natychmiast po zakończeniu nadawania stacja wprowadza nowy wolny znacznik, zaś z przełączeniem się w stan retransmisji oczekuje na odebranie końca własnej ramki (zasada odebrania własnej ramki jako pierwszej pozostaje tu nienaruszona). Strategia ta prowadzi do maksymalnego wykorzystania pasma sieci, lecz zysk ten w praktyce jest stosunkowo niewielki, a jednocześnie kontrola poprawności pracy sieci staje się utrudniona (jednoczesna transmisja wielu znaczników zajętych i co najwyżej jednego znacznika wolnego).

Minimalna długość pierścienia

Po nadaniu, wolny znacznik okrąża pierścień bez dalszej interwencji stacji (jest retransmitowany dookoła pierścienia). Z tego względu długość bitowa pierścienia musi

być taka by cały znacznik (wszystkie jego bity) mógł jednocześnie w nim przebywać. Długość bitowa pierścienia wyznaczana jest przez:
- opóźnienie w każdej stacji - np. 1 bit (część stała);
- długość toru transmisyjnego i szybkość transmisji (opóźnienie propagacji - część zmienna).

Aby umożliwić pracę sieci, złożonej zaledwie z dwóch stacji, połączonych bardzo krótkimi odcinkami medium, należy wprowadzić do sieci sztuczne opóźnienie, wynoszące np. 8 bitów (w rozwiązaniach prostych) czy 24 bity (w rozwiązaniu IBM Token Ring). Wprowadzenie takiego minimalnego opóźnienia do każdej stacji przekreśliłoby ważną zaletę omawianego typu MAC - dobre wykorzystanie medium, dlatego bufor opóźniający (rejestr przesuwający) włącza się tylko w jednej, wydzielonej stacji-monitorze, która pełni również rolę głównego zegara sieciowego oraz nadzoruje pracę sieci.

Usługi utrzymania sieci

W sieci typu token ring istnieją trzy główne typy sytuacji awaryjnych, które powinny być automatycznie rozpoznawane i obsługiwane:
- zagubienie wolnego znacznika (*ang. lost token*);
- wielokrotnie krążąca (nie usunięta) ramka (*ang. circulating frame*);
- dwa (lub więcej) wolne znaczniki w sieci (*ang. duplicate token*).

Sytuacje te mogą być obsługiwane w sposób rozproszony (odpowiedzialność za to spoczywa na każdej stacji) lub w sposób scentralizowany (wykrywa je stacja-monitor). Poniżej omówimy jedynie obsługę scentralizowaną, jako częściej spotykaną.

W wypadku stwierdzenia braku wolnego znacznika (upłynięcia maksymalnego czasu, w którym powinien zostać zaobserwowany wolny znacznik) stacja monitor "czyści" sieć (usuwa wszelkie ewentualne ramki) i ponownie wprowadza znacznik do sieci.

W razie nieusunięci ramki przez stację nadającą (w wyniku błędu) czyni to stacja-monitor. Do tego celu przewidziany jest w polu adresowym lub kontrolnym każdej ramki bit "monitor", zerowany przez stację nadającą, a ustawiany przez stację-monitor. Stacja-monitor ma obowiązek usunięcia z sieci każdej ramki, w której bit "monitor" jest ustawiony. W ten sposób żadna nie usunięta ramka nie będzie retransmitowana przez stację-monitor więcej, niż jeden raz.

Sytuację powielenia wolnego znacznika wykrywa każda stacja nadająca. Jeśli stacja taka stwierdzi, że podczas nadawania (lub tuż po jego zakończeniu) odbiera od stacji poprzedniej ramkę, której nie nadała (zaburzenia niezmiennika sieci), natychmiast kończy nadawanie i nie wprowadza nowego znacznika do sieci. W ten sposób sytuacja zbyt wielu znaczników przekształca się w brak znacznika, co jest obsługiwane przez stację-monitor w sposób opisany uprzednio.

Usługa typu broadcast

Przy source removal nadawanie do wszystkich stacji sieci odbywa się w naturalny sposób: adres broadcast, wspólny dla wszystkich stacji, pozwala każdej stacji na skopiowanie retransmitowanej ramki.

Potwierdzenie

Fakt obiegnięcia przez każdą nadaną ramkę całego pierścienia (i ponownego jej odebrania przez stację nadającą) pozwala na przysyłanie przez stację odbierającą potwierdzenia w ramach tej samej ramki. W tym celu, zwykle w sekwencji kończącej

ramkę, wydziela się sekwencję bitów służbowych, które mogą być ustawiane "w przelocie" (tak, jak zamiana znacznika wolnego na zajęty) przez stację odbierającą. Przykładowo bity te mogą mieć następujące znaczenie:

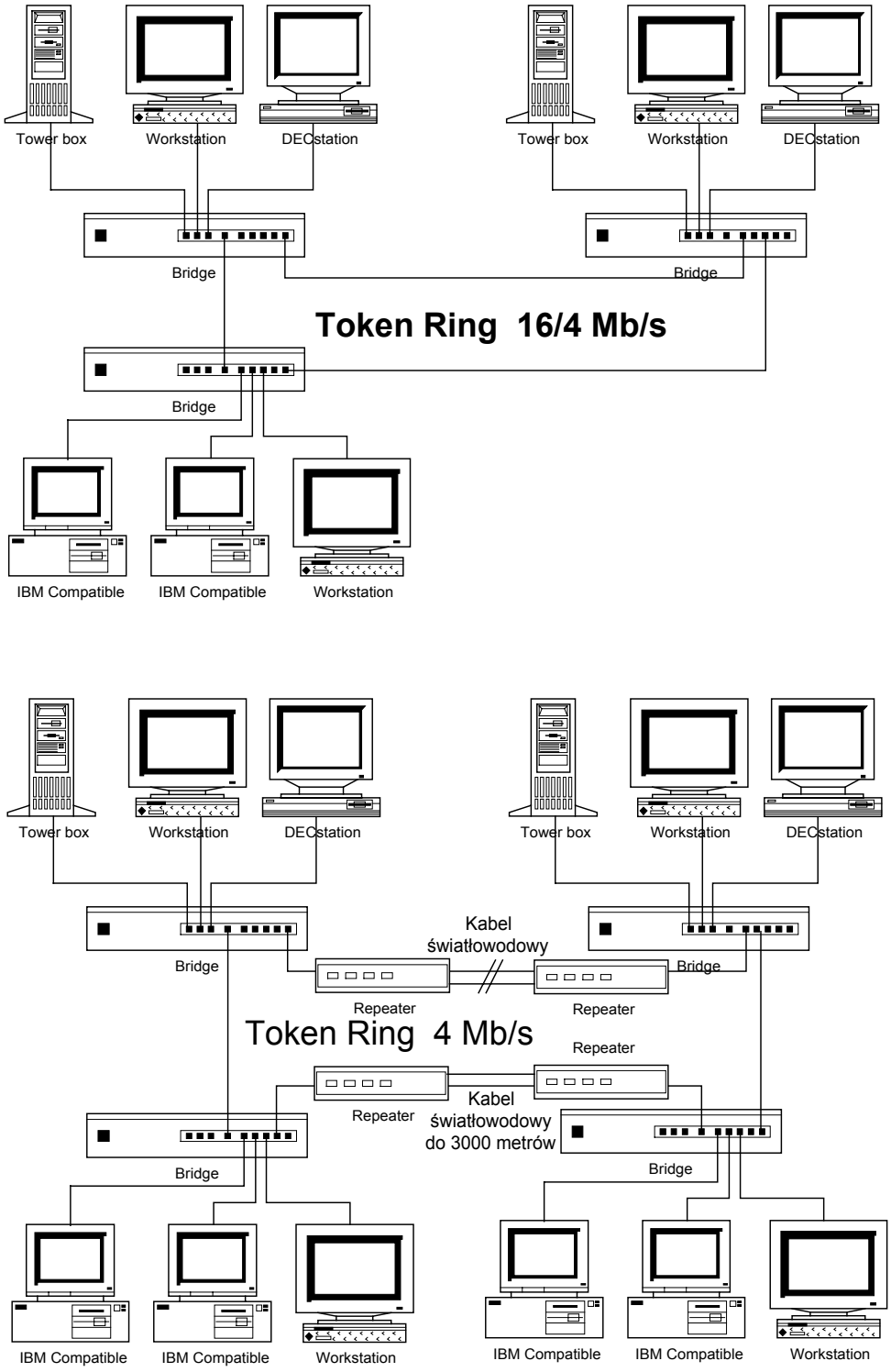
- adres rozpoznany (istnieje aktywna stacja o podanym adresie);
- ramka skopiowana (wykorzystana);
- błąd w ramce (ramka przekłamana).

W przypadku usługi broadcast do interpretacji dwóch pierwszych bitów służbowych należy dodać sformułowanie „przez co najmniej jedną stację". Bit błędu może (i powinien) być obsługiwany przez każdą retransmitującą stację. Przykładową strukturę sieci token ring przedstawiono na rysunku 3.19.

Przykład IBM Token Ring

Dane ogólne:

- Topologia: pierścień, z okablowaniem prowadzonym w układzie gwiazdy.
- Usuwanie ramek - source removal.
- Strategia wprowadzania znacznika - single token.
- Szybkość transmisji: 4 Mb/s, 16Mb/s.
- Medium transmisyjne: skrętka.
- Maksymalna ilość stacji: 260 (72 z tanim kablem telefonicznym).
- Automatyczna rekonfiguracja - izolowanie stacji uszkodzonych.
- Stacja-monitor: wybierana automatycznie (w wyniku rywalizacji), każdorazowo przy starcie sieci i po wystąpieniu poważnego błędu.
- Kodowanie transmisyjne: differential Manchester.
- 8 priorytetów.



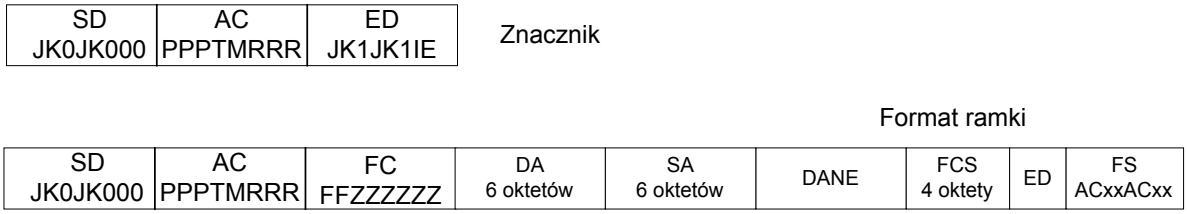
Rysunek 3.19 Struktura sieci token ring

Formaty ramek

Format znacznika i format ramki przedstawiono na rysunku 3.20.

Znacznik wolny od zajętego odróżnia wartość bitu T (token). Bit M (monitor) służy do usuwania ramki, która nie została usunięta przez stację nadającą (jak opisano wcześniej). Bity PPP wyznaczają aktualny priorytet znacznika wolnego. Bity RRR

umożliwiają rezerwację znacznika o podanym priorytecie. Elementy J i K są zaburzeniami kodu Manchester (nie jest to 0 ani 1), wyróżniającymi ciąg startowy (SDEL) i końcowy (EDEL) znacznika i ramki. Bit I (*ang. intermediate*) oznacza, że ramka należy do ciągu ramek, traktowanego jako całość. Bit E (*ang. error*) jest ustawiany przez każdą stację, która wykryje błąd (niezgodności wyniku kontroli nadmiarowej).



Rysunek 3.20 Format znacznika i ramki w sieci IBM Token Ring

Bajt FC (*ang. frame control*) określa, czy transmitowana ramka zawiera dane z wyższych warstw oprogramowania (ramka LLC), czy też jest to ramka służbowa, konieczna do realizacji zadań utrzymaniowych warstwy MAC (np. przesyłająca dane z warstwy SMT).

Adres stacji przeznaczenia DA (*ang. destination*) i źródła SA (*ang. source*) są sekwencjami 6-bajtowymi.

Pole danych może zawierać w szczególności 0 bajtów. Górna granica nie jest określona, lecz zależy od możliwości konkretnej implementacji. Standard określa, że każda realizacja powinna umożliwiać transmitowanie ramek o polu danych długości, co najmniej 133 bajtów

Czterobajtowe pole FCS (*ang. Frame Check Sequence*) umożliwia kontrolę poprawności przesyłanej ramki.

Pole FS (*ang. frame status*) zawiera bity potwierdzenia: A - adres rozpoznany, C - ramka skopiowana (wykorzystana). Bity te są powtórzone dwukrotnie, ponieważ pole nie jest objęte kontrolą kodową.

Zegar

Stacja - aktywny monitor (w odróżnieniu od pozostałych stacji, z których każda może stać się aktywnym monitorem w wyniku rywalizacji) zadaje szybkość transmisji za pomocą generatora kwarcowego. Pozostałe stacje pierścienia odzyskują przebieg zegarowy z transmitowanego przebiegu danych, za pomocą układów PLL. Połączone łańcuchowo układy PLL wprowadzają drżenie fazy (jitter), które powoduje, że chwilowa długość bitowa pierścienia może się zmieniać w zakresie +/- 3 bitów (przy szybkości transmisji 4 Mbit/s i maksymalnej ilości stacji równej 260). W stacji-monitorze włączony jest rejestr opóźniający (gwarantujący krążenie znacznika) o długości fizycznej 30 bitów, z czego 24 przypada na długość znacznika, a 6 - na korygowanie chwilowej długości bitowej pierścienia. Początkowo ustawiana jest długość logiczna rejestru równa 27 bitów. Monitor wybierany jest przy użyciu procedury rywalizacji adresów, opisanej wcześniej. Ramki, służące do realizacji tej procedury, są ramkami typu MAC (odpowiednia wartość pola FC).

Priorytety

Przy korzystaniu tylko z jednego, najniższego priorytetu (000), protokół dostępu nie odbiega od wcześniej opisanego.

Rekonfiguracja

Stacje są dołączane do sieci za pośrednictwem przekaźników, znajdujących się w "jądrze" sieci. Przekaźniki są zasilane indywidualnie przez stacje. Zanik napięcia (w wyniku uszkodzenia stacji lub na jej polecenie) odłącza stację i zwiera pierścień w miejscu jej dołączenia. Taka czynność może doprowadzić (i zwykle prowadzi) do chwilowego rozsynchronizowania się pierścienia i zapewne do utraty ramki. Pełna sprawność sieci przywracana jest automatycznie.

Slotted ring

Uwaga: w pierścieniu szczelinowym stosuje się zasadę usuwania ramki przez stację nadającą (source removal).

Zasada działania

"Długość bitowa" pierścienia o szybkości transmisji 10 Mbit/s, 100 stacjach i odległości pomiędzy stacjami równej 10 m wynosi nieco ponad 150 bitów. W pierścieniu szczelinowym długość ta podzielona jest na stalą liczbę niewielkich ramek (np. 4 ramki po 38 bitów, jak w Cambridge Ring), zwanych również szczelinami lub mini pakietami. Ramki te, których struktura ustalana jest na wstępie przez stację-monitor, stale obiegają pierścień. W rozwiązaniu podstawowym każda ramka ma taki sam format, choć nie jest to absolutnie konieczne z punktu widzenia protokołu dostępu do medium. Każda ramka składa się przynajmniej z bitu "wolna/zajęta" (na początku ramki) i pola danych. Dąży się do minimalizowania opóźnienia retransmisji - minimalne teoretyczne opóźnienie w każdej stacji wynosi 1 bit. Bit "wolna/zajęta" pełni rolę podobną do znacznika w sieci token ring, jednakże w omawianym rozwiązaniu w sieci występuje jednocześnie wiele znaczników. Najważniejszą różnicą koncepcyjną jest to, że wszelkie operacje związane z nadawaniem-usuwaniem ramek dokonywane są tu na zasadzie modyfikacji wartości retransmitowanego bitu (w żadnej chwili nie dokonuje się rozłączenia odbiornika i nadajnika stacji).

Nadawanie

Stacja pragnąca nadawać oczekuje na odebranie ze stacji poprzedniej początku ramki oznaczonej jako wolna. Następnie, w przelocie zmienia wartość bitu zajętości na "zajęta", po czym modyfikuje zawartość pola danych, ustawiając bity zgodnie z treścią nadawanej ramki. Po zakończeniu nadawania stacja oczekuje na obiegnięcie pierścienia przez ramkę. W chwili, gdy odbiera bit zajętości własnej ramki, ustawia jego wartość ponownie na "wolna". W ten sposób "usuwa" się ramkę; usuwania fizycznego nie dokonuje się. Rozpoznawanie własnej ramki prowadzone jest na zasadzie zliczania retransmitowanych ramek, gdyż oczywiście nie obowiązuje tu reguła zgodnie, z którą pierwsza odebrana ramka jest ramką własną (wręcz przeciwnie - to z reguły nie jest ramka własna). Zliczanie ramek możliwe jest dzięki zachowywaniu stałej struktury transmisji w pierścieniu. Stacja może ponownie nadawać (starać się przejąć szczelinę) dopiero po oznaczeniu uprzednio nadanej ramki jako wolnej. Dzięki temu unika się niebezpieczeństwa zmonopolizowania pierścienia przez jedną stację.

Odbiór

Zaadresowana stacja kopiuje retransmitowaną ramkę do wewnętrznych buforów. Stacja może również umieszczać przy końcu ramki potwierdzenie (negatywne lub pozytywne), które zostanie następnie odczytane przez stację źródłową Nadawanie i odbiór ramek z adresem okólnikowym nie wymaga żadnych specjalnych zabiegów.

Stacja-monitor

Stacja-monitor (zwykle wybrana na stałe) może wypełniać następujące zadania:

- zadawać szybkość transmisji, śledzoną następnie przez inne stacje za pomocą układów PLL;
- wydłużać pierścień do wymaganej długości za pomocą rejestru przesuwnego;
- usuwać ramki, które nie zostały oznaczone jako wolne (korzystając z wartości bitu "monitora", w sposób omówiony uprzednio).

Wady i zalety

Sieć typu slotted ring jest przedmiotem standardów międzynarodowych, jednakże Cambridge Ring pełni rolę de facto standardu. Sieć jest popularna w przemyśle. Zapewnia znany i krótki czas dostarczenia wiadomości, lecz wykorzystanie pasma jest słabe (długość pola danych jest mała w porównaniu z długością ramki). Powoduje to również konieczność rozbijania pakietów użytkowych na minipakiety w wyższych warstwach oprogramowania.

Token bus - szyna z przesyłaniem znacznika

Sieć typu token bus jest przykładem sieci o topologii szynowej (ogólnie - drzewa), lecz o nielosowej, deterministycznej zasadzie dostępu na żądanie.

Zasada działania

Stacjom, dołączonym do szyny, przydziela się unikalne adresy. W sieci transmitowane są dwa rodzaje ramek: ramki użytkowe i znacznik (token). Pod względem funkcjonalnym procedura dostępu przypomina token ring - tworzy się pierścień logiczny, w którym każda stacja zna numer stacji poprzedniej i następnej (w żaden sposób nie związany z fizycznym rozmieszczeniem stacji). Jednakże, odmiennie niż w sieci o topologii pierścienia, w sieci token bus znacznik nie krąży autonomicznie i nie jest "przekłamywany" w trakcie retransmisji, lecz jest wysyłany w sposób jawny, jak pozostałe ramki użytkowe.

Podobnie jak w innych sieciach o topologii szyny, każdą transmisję ramki poprzedza nadawanie preambuły synchronizacyjnej. Nie ma zatem problemu z utrzymywaniem synchronicznej pracy sieci (co ma miejsce w sieciach pierścieniowych).

Nadawanie

Stacja "posiadająca" znacznik ma prawo do nadawania (przez określony czas) ramek, adresowanych do dowolnej innej stacji sieci. Gdy stacja ta nie korzysta z prawa nadawania lub też gdy czas przeznaczony na nadawanie upłynie, ma ona obowiązek jawnie wysłać ramkę-znacznik do stacji logicznie kolejnej, która tym samym stanie się uprawniona do nadawania. Dzięki takiej regulacji dostępu, w medium nie zachodzą kolizje podczas normalnej pracy sieci.

Dołączanie logiczne nowych stacji

Każda stacja B ma obowiązek, co określony czas (zwykle co kilka minut) wysyłać ramkę zaproszenia do włączenia się nowej stacji do sieci. Ramkę-zaproszenie wysyła się na normalnych zasadach, opisanych powyżej. Ramka ta zawiera adres stacji wysyłającej B i stacji logicznie następnej E. Tylko stacje jeszcze nie włączone w pierścień logiczny i oznaczone adresem leżącym wewnątrz podanego zakresu mogą odpowiedzieć na zaproszenie. Ponieważ stacje te nie posiadają znacznika, nadawane przez nie ramki odpowiedzi mogą uczestniczyć w kolizji. Do rozstrzygania kolizji stosuje się procedurę rywalizacji adresów:

- Stacja nadająca zaproszenie B oczekuje na odpowiedź przez kwant czasu równy dwukrotnemu maksymalnemu opóźnieniu transmisyjnemu
- Jeśli przez ten czas nie nadejdzie żadna odpowiedź stacja zapraszająca kontynuuje normalną pracę.
- Jeśli nadejdzie odpowiedź od jednej stacji C, stacja B modyfikuje przechowywany adres stacji następnej (zmienia jego wartość z E na C), po czym przesyła znacznik do stacji C, która tym samym została włączona w pierścień logiczny. Stacja C zna już adres swego poprzednika B i następnika E (z zawartości pierwotnej ramki zapraszającej).
- Jeśli odpowiedź zostanie wysłana jednocześnie przez dwie lub więcej stacji (np. C i D), stacja zapraszająca B stwierdzi zajście kolizji. Stacja B wysyła ramkę "rozwiązania konfliktu", po czym oczekuje 4 kwanty czasu.

Każdy kwant czasu odpowiada innej kombinacji dwóch najbardziej znaczących bitów adresu stacji, ubiegających się o włączenie do pierścienia, np.:

- 11- kwant pierwszy;
- 10 - kwant drugi;
- 01 - kwant trzeci;
- 00 - kwant czwarty.

Stacja o dwóch pierwszych bitach adresu 11 odpowiada w kwancie pierwszym, o bitach 01 - w trzecim itd. Jeśli stacja o adresie niższym stwierdzi transmisję we wcześniejszym kwancie czasu, wstrzymuje się od nadawania (jest wyłączona z procedury rywalizacji w bieżącej turze).

- Dwie stacje o różnych adresach, lecz identycznych dwóch początkowych bitach adresu nadadzą ramkę w tym samym kwancie, co oczywiście doprowadzi do kolizji. Po stwierdzeniu kolizji, stacja zapraszająca ponownie wysyła ramkę "rozwiązania konfliktu" i ponownie oczekuje przez cztery kwanty na odpowiedź. Tylko stacje, które nadały odpowiedź w pierwszej fazie, mają prawo do dalszego ubiegania się o włączenie do pierścienia logicznego. Tym razem jednak kwanty czasu przyporządkowane są dwóm kolejnym bitom adresu.
- W razie ponownego wystąpienia konfliktu, procedurę powyższą powtarza się dla dwóch kolejnych (mniej znaczących) bitów adresu. Unikalne adresy stacji gwarantują, że procedura zakończy się sukcesem (dokładnie jedna stacja nada pomyślnie odpowiedź). Stacja ta zostanie włączona do pierścienia logicznego w opisany wcześniej sposób.

Inicjalizacja pracy sieci

Procedura inicjalizacji przeprowadzana jest, jeśli przez ustalony czas stacje stwierdzą brak aktywności sieci (czyli w wypadku włączenia sieci lub zagubienia znacznika). Procedura ta opiera się na zasadzie rywalizacji adresów, podobnie jak przy dołączaniu nowej stacji. Stacja, która "wygra" rywalizację, ma prawo nadać znacznik.

Odłączanie logiczne stacji

Stacja może zostać usunięta z pierścienia logicznego z własnej inicjatywy lub przez stację poprzednią (w razie uszkodzenia).

Stacja B, pragnąca odłączyć się z własnej inicjatywy, oczekuje na otrzymanie znacznika ze stacji poprzedniej A, a następnie odsyła znacznik ponownie do stacji A, informując ją również o adresie własnego następnika C. Stacja A zmienia adres swego następnika z B na C i przesyła znacznik do stacji C. Stacja B może się ponownie włączyć do sieci w sposób opisany uprzednio.

Stacja A, po przesłaniu znacznika do swego następnika B, prowadzi przez krótki czas (kilka, np. 4 kwanty) nasłuch medium. Jeśli stacja ta stwierdzi, że B nie wykazuje aktywności (nie nadaje ramki lub znacznika), ustala adres kolejnego następnika (np. przy zastosowaniu procedury rywalizacji adresów), modyfikuje adres następnika i przesyła do niego znacznik Stacja B tym samym zostaje odłączona od pierścienia logicznego.

Powielenie znacznika

Jeśli stacja, która otrzymała znacznik, stwierdzi, że w medium toczy się inna transmisja (czyli, że istnieje drugi znacznik), natychmiast zaprzestaje nadawania. Jeśli w wyniku tego ilość znaczników spadnie do 0, normalna praca sieci jest przywracana w procedurze inicjalizacji.

Długość ramki

W sieci token bus ograniczenie z góry na długość ramki wynika wyłącznie z potrzeb aplikacji (ograniczenia fizycznego brak). Z powodu braku konfliktów (w trakcie normalnej pracy) nie ma również ograniczenia na długość minimalną.

Przykład - IEEE 802.4 token bus

Podstawowe dane:

- Szybkość transmisji: 1 Mbit/s, 5 Mbit/s, 10 Mbit/s.
- Pasmo: Baseband lub broadband.
- Całkowita długość ramki: max. 8191 bajtów.

Na rysunku 3.21 przedstawiono format ramki w sieci IEEE 802.4 Token Bus.

Format ramki

PREAMBUŁA	SDEL	FC FFMMMPPP	DA 6 oktetów	SA 6 oktetów	DANE	FCS 4 oktety	EDEL 1 oktet

Rysunek 3.21 Format ramki w sieci IEEE 802.4 Token Bus

Sieci tego typu znajdują specjalistyczne zastosowanie w przemyśle, ze względu na zdeterminowany czas dostępu do medium.

3.4 Porównanie właściwości sieci

Porównanie właściwości dotyczyć będzie cech i zagadnień konstrukcyjnych, wynikających bezpośrednio z przyjęcia topologii pierścienia lub szyny (drzewa) i z wynikającej z wybranej topologii zasady dostępu do medium.

Zagadnienia transmisyjne - pierścień

Cechą pierścienia jest wykorzystywanie każdego odcinka medium przez tylko jeden nadajnik (transmisja punkt-punkt). Stacje pełnią rolę cyfrowych regeneratorów sygnału. Osiągnięcie odległości transmisji pomiędzy dwiema stacjami rzędu setek metrów nie przedstawia żadnych trudności, nawet przy wykorzystaniu skrętki jako medium. Wprowadzane przez długie odcinki medium opóźnienie transmisyjne nie wpływa bezpośrednio na działanie protokołu dostępu, a jedynie może zwiększyć czas oczekiwania na nadanie ramki. Tym samym technicznie możliwe (i bardzo proste) jest zbudowanie pierścienia o promieniu np. 10 kilometrów.

Charakter transmisji w pierścieniu umożliwia również stosowanie kabli światłowodowych całkowicie odpornych na zakłócenia, co może mieć podstawowe znaczenie w sieciach przemysłowych.

Zagadnienia transmisyjne - szyna

W sieci o topologii szyny lub drzewa (i o protokole dostępu typu CSMA/CD) występuję wiele czynników natury technicznej ograniczających jej rozmiary (rozpiętość i rozmieszczenie stacji).

Konieczność wykrywania kolizji przez stację nadającą (porównanie silnego sygnału własnego ze słabym sygnałem odległym) sprawia, że maksymalne tłumienie sygnału nie może przekroczyć określonej wielkości (w pierścieniu dopuszczalne jest tłumienie bardzo duże, ograniczone jedynie czułością odbiornika, odbierającego pojedynczy sygnał).

Dołączone równolegle nieaktywne nadajniki wprowadzają do sieci szum analogowy, utrudniający działanie odbiorników - ograniczenie na liczbę stacji w segmencie.

Złącza (penetrujące lub BNC) wprowadzają do medium nieciągłości, będące powodem odbić. W celu minimalizacji tych odbić konieczne są ograniczenia w rozmieszczeniu stacji (np. nie bliżej, niż co 2,5 metra). Poza ograniczeniami technicznymi, podstawowym ograniczeniem logicznym jest konieczność zapewnienia odpowiedniej sprawności protokołu dostępu. Wydłużanie medium powoduje wydłużanie okna kolizji i spadek sprawności protokołu (przy stałej długości ramki). Zwiększenie szybkości transmisji przy stałej długości medium powoduje ten sam efekt, przez skrócenie czasu nadawania ramki. Taka zależność od szybkości transmisji nie występuje w sieciach pierścieniowych.

Powyższe rozważania sugerują, że sieci pierścieniowe znacznie lepiej znoszą wydłużanie i zwiększanie szybkości transmisji, niż sieci o topologii szyny.

Synchronizacja - pierścień

W pierścieniu wymagane są specjalne zabiegi służące do utrzymania synchronizacji poszczególnych stacji. Możliwe sposoby realizacji tych zabiegów przedstawione są poniżej.

Układ PLL aktywny jest w każdej stacji - praca na częstotliwości własnej

- Zegar odbiorczy każdej stacji wytwarzany jest przez układ PLL. Kwarcowy zegar nadajnika pracuje na ustalonej częstotliwości. W każdej stacji niezbędny jest bufor elastyczny.
- Każda stacja posiada dwa układy PLL: odbiorczy i nadawczy.
- Jedna stacja nadaje i retransmituje dane, używając do tego celu generatora kwarcowego. Pozostałe stacje śledzą częstotliwość zegarową za pomocą układów PLL, wytwarzających wspólny, odbiorczy i nadawczy przebieg zegarowy. Bufor niezbędny jest tylko w jednej stacji ("aktywny monitor").
- Transmisja bitów następuje asynchronicznie.

Bufor lub bufory służą do zniwelowania zjawiska drżenia fazy (jitter), powstającego w wyniku zniekształcenia (pochylenia) zboczy przebiegu w medium. Drżenie fazy akumuluje się przy łańcuchowym połączeniu nadajników i odbiorników, prowadząc do chwilowych zmian długości bitowej pierścienia (w granicach kilku bitów). Zjawisko jitteru ogranicza maksymalną ilość stacji (odcinków medium) do ok. 260.

Bufory elastyczne niezbędne są również z uwagi na konieczność utrzymania minimalnej (token ring) lub określonej (slotted ring) długości bitowej pierścienia.

Synchronizacja - szyna

Powyższe zjawiska nie występują. Synchronizacja wymagana jest jedynie w trakcie transmisji ramki. Nadawanie następuje każdorazowo z szybkością określoną przez kwarcowy zegar nadawczy stacji nadającej. Każda nadawana ramka musi być poprzedzona preambułą synchronizacyjną, umożliwiającą układom PLL odbiorników wytworzenie poprawnego przebiegu zegara odbiorczego. Preambuła synchronizacyjna ma zwykle długość kilku bajtów (strata przepustowości), choć w eksperymentalnej wersji sieci Ethernet z powodzeniem stosowano bardzo krótką preambułę 1-bitową.

Izolacja elektryczna - pierścień

Z uwagi np. na prądy błądzące nie jest możliwe galwaniczne połączenie stacji pierścienia o średnicy przekraczającej kilkanaście metrów. Każdy odcinek medium musi być odseparowany obustronnie lub jednostronnie, za pomocą optoizolatora lub transformatora. Izolacja taka zapewniana jest automatycznie w wypadku użycia medium światłowodowego.

Izolacja elektryczna - szyna

Z analogicznych powodów, ekran kabla symetrycznego musi pozostać niezmieniony lub zostać uziemiony dokładnie w jednym miejscu (uziemienie to powinno wytrzymywać przepływ prądu rzędu 2500 A). Kabla nie wolno prowadzić na zewnątrz budynku, bo mogłoby posłużyć jako piorunochron.

Nadajnik-odbiornik jest sprzężony galwanicznie z kablem, lecz musi być odseparowany (transformatorowo lub pojemnościowo) od pozostałych układów stacji.

Niezawodność - Pierścień

Popularne przekonanie, że sieć pierścieniowa jest z definicji bardziej zawodna od sieci o topologii szyny, nie znajduje uzasadnienia.
Istnieją dwa główne sposoby zapewnienia niezawodności sieci:

- automatyczne odłączanie stacji i zwieranie miejsca jej dołączenia za pomocą przekaźnika jak w sieci IBM Token Ring;
- dwa pierścienie przeciwbieżne, umożliwiające rekonfigurację sieci w razie uszkodzenia odcinka medium lub stacji (z inicjatywy stacji uszkodzonej lub nawet bez jej zgody) jak to ma miejsce w sieci FDDI.

W drugim rozwiązaniu, algorytm rekonfiguracji pierścienia umożliwia nawet, w wypadkach katastrofalnych, rozpadnięcie się sieci na pewną ilość niezależnych, mniejszych sieci, z których każda zachowuje zdolność do pracy. Przywrócenie pierwotnego składu sieci następuje automatycznie, po usunięciu uszkodzenia. Trzeba jednak stwierdzić, że algorytm rekonfiguracji jest dość skomplikowany, a jego wykonanie może być długotrwałe.

W sieci pierścieniowej stacja, która jako pierwsza wykryje błąd postaci ramki, może wnioskować o uszkodzeniu stacji poprzedniej lub łączącego te dwie stacje odcinka medium. Lokalizacja uszkodzeń może być zatem włączona do procedur utrzymaniowych oprogramowania stacji.

Niezawodność - szyna

Pasywne medium jako takie (kabel współosiowy) jest bardzo niezawodne. Każda stacja może jednak doprowadzić do awarii całej sieci, przez:

- zwarcie do stałego potencjału w miejscu dołączenia stacji, co całkowicie uniemożliwia nadawanie przez inne stacje - brak skutecznej obrony;
- długotrwałą, niekontrolowaną aktywność stacji (jabber) - układ "anti jabber" odłącza nadajnik po upływie maksymalnego, ustalonego czasu nadawania.

W żadnym wypadku nie jest możliwa jakakolwiek rekonfiguracja topologiczna. Znajdowanie miejsca uszkodzenia kabla współosiowego (np. zagięcia, zagniecenia lub przerwania) wymaga zastosowania reflektometru. Ma on często postać urządzenia zewnętrznego, którego praca wyklucza równoczesną pracę sieci. Niektóre układy scalone sterowników sieci dysponują wbudowanymi funkcjami reflektometru w dziedzinie czasu (ustalającego miejsce awarii na podstawie pomiaru opóźnienia sygnału odbitego).

Niedeterminizm

Zasada losowego dostępu do medium (szyna) nie gwarantuje określanego, maksymalnego czasu oczekiwania na pomyślne nadanie ramki (z uwagi na kolizje). Jednakże, przy odpowiednio małym obciążeniu sieci, prawdopodobieństwo zbyt długiego oczekiwania jest bardzo niewielkie. W szczególności, prawdopodobieństwo to może być mniejsze, niż prawdopodobieństwo błędu w sieci pierścieniowej, powodującego konieczność przeprowadzenia długotrwałej procedury rekonfiguracji. Sieci pierścieniowe, z procedurą dostępu na żądanie, są deterministyczne (zapewniają znany, maksymalny czas oczekiwania), dlatego preferowane są do zastosowań przemysłowych, do kontroli procesów technologicznych nie tolerujących nieterminowego dostarczania sygnałów sterujących (np. procesy chemiczne czy jądrowe). Determinizm ten dotyczy wszakże zjawisk, związanych z normalną, sprawną pracą sieci. W ogólności, oba typy sieci (czy raczej ich implementacje) są niedeterministyczne. Trzeba jednak powiedzieć, że ramki dostarczane są z prawdopodobieństwem bardzo bliskim jedności.

3.5 Łączenie sieci

Łączenia sieci dokonuje się, gdy:

- z potrzeb użytkownika wynika konieczność zwiększenia ilości stacji sieci ponad granicę, wyznaczoną przez parametry konkretnej, używanej sieci lokalnej;
- połączenia za pomocą sieci lokalnej wymagają dwie lub kilka grup użytkowników z których każda oddalona jest od pozostałych użytkowników na odległość, przekraczającą maksymalną odległość transmisji w pojedynczej sieci;
- należy scalić w jedną logiczną całość dwie (lub więcej) dotychczas użytkowane sieć lokalne;
- stacje sieci lokalnej wymagają dołączenia do sieci rozległej WAN.

W zależności od konkretnych potrzeb, do łączenia sieci używa się następujących urządzeń (systemów):

- repeater (regenerator);
- bridge (pomost);
- router;
- gateway (brama).

Repeater

Repeater łączy dwa segmenty sieci lokalnej tego samego typu na poziomie warstwy fizycznej. Służy do rozszerzenia obszaru, obsługiwanego przez sieć. Przykładowo, za pomoc tego typu urządzeń można łączyć segmenty (maksymalnie 500-metrowe) sieci Ethernet aż do uzyskania maksymalnej rozpiętości sieci, równej 2.5 km.

Bridge

Bridge łączy sieci na poziomie warstwy MAC (w ogólności - na poziomie warstwy łącza danych w strukturze ISO/OSI) rysunek 3.22. Należy zauważyć, że rysunek pokazuje jedynie dwie łączone sieci - może ich być więcej.

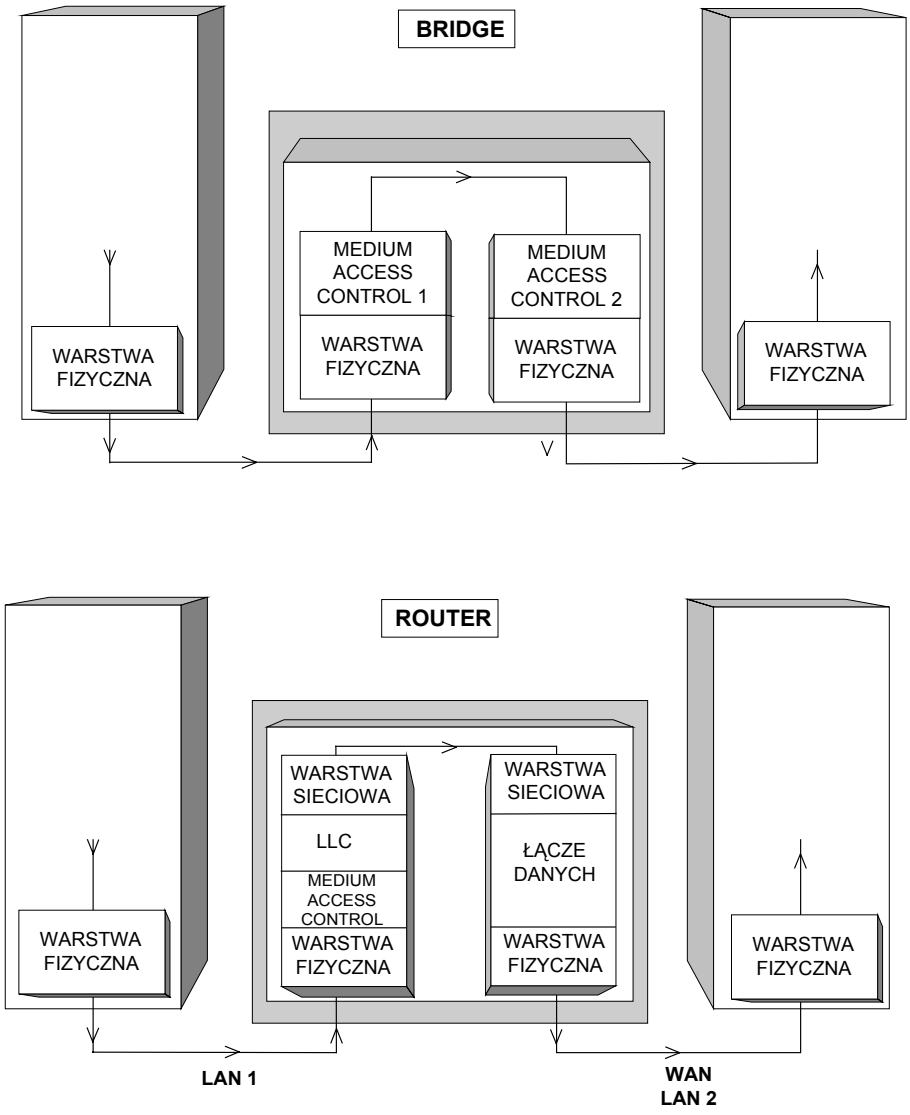
Struktura oprogramowania sieciowego (wyższych warstw architektury) musi być we wszystkich łączonych sieciach identyczna, zaś format ramek - zbliżony W szczególności: struktura pól adresowych i pola danych musi być identyczna. Bridge przesyła ramkę do sąsiedniej sieci, jeśli stwierdzi, że zawarty w ramce adres stacji przeznaczenia dotyczy stacji, znajdującej się w tej drugiej sieci. W tym celu bridge wypełnia (w drodze obserwowania aktywności wszystkich łączonych sieci) tablicę adresów stacji dołączonych do każdej z sieci. Nie dokonuje się natomiast żadnego przekodowania adresów w transferowanych ramkach. Przestrzeń adresowa połączonych sieci traktowana jest jako jednorodna, czyli nie mogą występować dwa identyczne adresy. Działanie pomostu jest przezroczyste z punktu widzenia użytkowników sieci i nie wymaga żadnych akcji z ich strony.

Zaznaczone na rysunku połączenie dwóch "części" pomostu może również być zrealizowane za pomocą np. łącza mikrofalowego, co pozwala na łączenie sieci fizycznie dość znacznie oddalonych od siebie.

Router

Router (rysunek 3.22) łączy sieci na poziomie warstwy sieciowej. Router nie jest przezroczysty dla wyższych warstw architektury. Jego zadania to m.in. translacja adresów i zmiana wielkości pakietów (fragmentacja i składanie pakietów). Za jego pomocą można:

– kierować pakiety do sąsiedniej sieci LAN za pośrednictwem sieci pakietowej WAN;
– łączyć sieci lokalne o różnych maksymalnych długościach pola danych ramki.



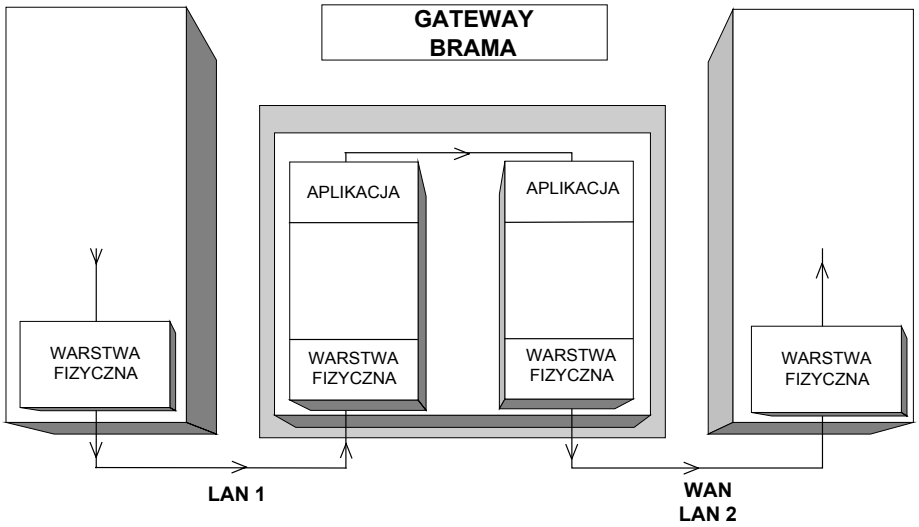
Rysunek 3.22 Łączenie sieci za pomocą bridgea i routera

Gateway

Gateway (rysunek 3.23) służy do łączenia sieci u radykalnie różnych zestawach protokołów. Połączenie następuje na poziome warstwy aplikacji. Każda z "połówek" bramy odpowiada swoją architekturę strukturze danej sieci, zaś wspólną płaszczyznę stanowią usługi (programy transferu danych) wykorzystujące warstwę aplikacji.

Gateway stanowi potencjalne wąskie gardło sieci. Ponadto, zbiór usług, świadczonych użytkownikom obu sieci, jest predefiniowany (na poziomie aplikacji), a

tym samym sztywny. Należy zauważyć, że spotyka się również inne określenie bramy (zwłaszcza w dokumentach ISO), jako systemu łączącego sieci na poziomie warstwy sieciowej, jak uprzednio opisany router).



Rysunek 3.23 Łączenie sieci za pomocą gatewaya

4 Sieci miejskie

4.1 FDDI

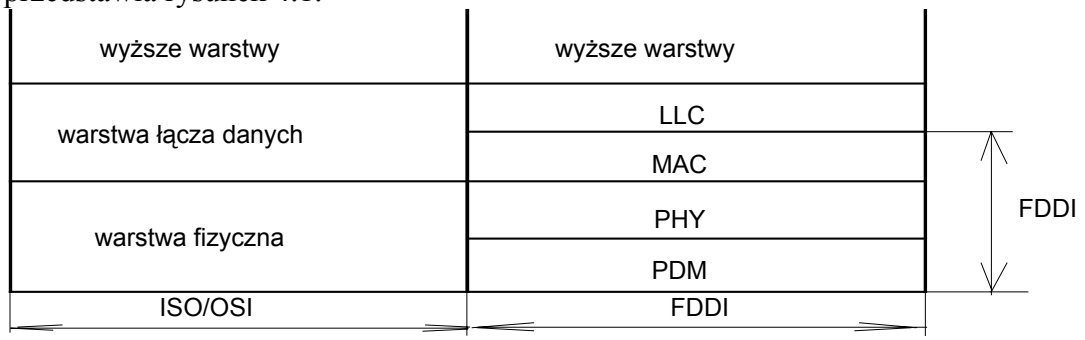
Charakterystyka i model odniesienia dla sieci FDDI

Sieciowy standard FDDI opracowany został w ramach prac amerykańskiej organizacji standaryzacyjnej ANSI. Sukces FDDI potwierdził fakt zaakceptowania opracowań ANSI, praktycznie bez poprawek i zmian, przez międzynarodową organizację standaryzacyjną ISO. Sieć FDDI jest klasyfikowana zwykle jako sieć lokalna.

FDDI w wersji podstawowej określa cztery specyfikacje protokołów dla następujących warstw:

- PMD - Physical layer Medium Dependent;
- PHY - PHYsical layer protocol;
- MAC - Medium Access Control;
- LLC - Logical Link Control

Wzajemne usytuowanie warstw względem siebie oraz modelu odniesienia OSI przedstawia rysunek 4.1.



Rysunek 4.1 Usytuowanie warstw FDDI w stosunku do modelu ISO

Sieć FDDI w zamyśle twórców miała być tanią, światłowodową, szybką siecią transmisji danych o charakterze lokalnym. Jednakże użytkownicy i producenci operujący na rynku usług teleinformatycznych bardzo szybko zauważyli i wykorzystali szereg zalet FDDI, pozwalających na stosowanie sieci w charakterze sieci miejskiej MAN. W chwili obecnej zdecydowana większość sieci FDDI pracuje jako sieci miejskie lub sieci "podkładowe" (backbone) dla wolniejszych sieci lokalnych (Ethernet, Token Bus, Token Ring).

Sieć FDDI pracuje z szybkością 100 Mbit/s, transmisja w poszczególnych pętlach tj. pierwotnej i wtórnej odbywa się w przeciwnych kierunkach. W normalnych warunkach sieć wykorzystuje do transmisji danych tylko pętlę pierwotną. Pętla wtórna podlega jedynie stałej kontroli i pomiarom i stanowi rezerwę na wypadek fizycznego uszkodzenia medium transmisyjnego. W takim wypadku sieć ulega automatycznej rekonfiguracji, po usunięciu awarii sieć automatycznie powraca do stanu pierwotnego (patrz rozdział pt. niezawodność sieci). FDDI pracuje efektywnie i poprawnie, gdy całkowite obciążenie nie jest wyższe od 80%, powyżej tego progu sieć wchodzi w stan przeciążenia i pojawić się mogą niedogodności odczuwane przez niektórych użytkowników. W pojedynczej sieci FDDI może znaleźć się maksymalnie 500 stacji sieciowych (ograniczenie ze względu na opóźnienie wprowadzane przez stacje, które nie może być większe niż 1512 ns), maksymalna łączna długość wszystkich odcinków

światłowodu w sieci nie może przekroczyć 200 km (ograniczenie ze względu na opóźnienie sygnału wnoszone przez medium transmisyjne, przy szybkości propagacji sygnału równej 5085 ns/km daje maksymalne opóźnienie sygnału 1.017 ms). Suma opóźnień propagacyjnych i opóźnień wnoszonych przez stacje dla maksymalnie skonfigurowanej sieci wynosi:

$$(500 \times 1512ns) + 1{,}017ms = 1{,}773ms$$

Protokół dostępu do medium w sieci FDDI nazywany jest protokołem opóźnionego lub inaczej czasowo ograniczonego tokenu (*ang.timed token rotation protocol*).

Polega on na tym, że stacja maże prowadzić transmisję jedynie w chwili posiadania tokenu - ramki o specjalnym formacie transmitowanej pomiędzy wszystkimi stacjami sieci. Czas przez który stacja może przetrzymywać token (a więc prowadzić transmisję w danym obiegu tokenu) regulowany jest wartościami dwóch zegarów stacji TRT (*ang. Token Rotation Timer*) i THT (*ang. Token Holding Timer*).

Protokół FDDI wyróżnia dwa rodzaje transmisji:

- synchroniczna-charakteryzuje się deterministycznie określonym:
  - minimalnym czasem uzyskania dostępu do medium;
  - stałą dla danej stacji przepływnością;
  - wielkości te ustalane są w drodze negocjacji z operatorem sieci.
- asynchroniczna - charakteryzuje się niedeterministycznym przydziałem medium, przepływność w medium przydzielana jest stacjom dynamicznie w zależności od aktualnego obciążenia sieci.

Transmisja synchroniczna charakteryzowana jest dwoma parametrami:

- czasem zajętości medium (określa maksymalny czas, przez jaki stacja może przetrzymywać token)
- częstością dostępu do medium - maksymalny czas obiegu tokenu w pętli TTRT (*ang. Target Token Rotation Time*).

Transmisja asynchroniczna kontrolowana jest przez dwa różne mechanizmy w zależności od rodzaju aktualnie krążącego tokenu w sieci.

Standard definiuje następujące rodzaje tokenu:

- zastrzeżony, dla przydziału całości przepływności wykorzystywanej dla transmisji asynchronicznej dwóm stacjom prowadzącym intensywną wymianę;
- niezastrzeżony, zapewnia "sprawiedliwy" podział przepływności pomiędzy wszystkich użytkowników sieci.

Topologia sieci

FDDI pracuje w układzie podwójnej pętli. Wszystkie węzły dołączone do pętli zdolne są do transmisji danych w niezależnych pętlach światłowodowych, w przeciwnych kierunkach. Do medium dołączane są dwa rodzaje węzłów:

- DAS (*ang. Dual Attachment Station*);
- DAC (*ang. Dual Attachment Concentrator*).

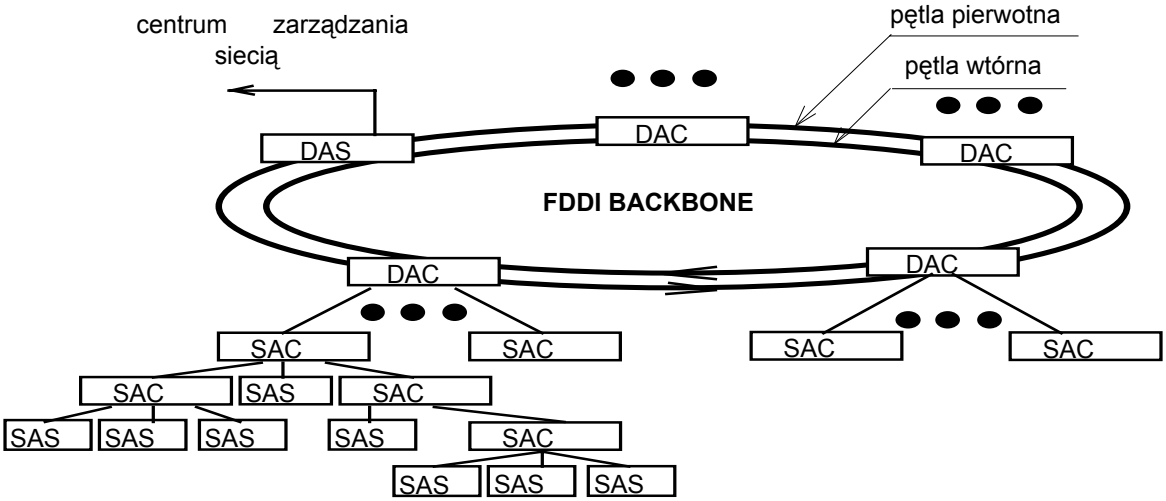
DAS pełni rolę bezpośredniego koncentratora użytkowników, zaś DAC koncentratora stacji sieciowych o prostszej budowie (zaletą tego rozwiązania jest obniżenie kosztów budowy sieci).

Stacje podłączane do DAC to:

- SAS (*ang. Single Attachment Station*) stacja do której bezpośrednio dołączani są abonenci;

– SAC (*ang. Single Attachment Concentrator*) stacja kolejnego poziomu koncentracji.

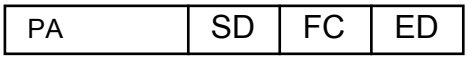
Stosowanie wielu poziomów koncentracji w sieci FDDI prowadzi do powstania sieci o strukturze podwójnej pętli z drzewami (*ang. dual ring of trees*) (rysunek 4.2). Zaletą tego typu topologii jest duża elastyczność w zakresie rozbudowy sieci, zwiększona niezawodność (większość awarii i przestojów sieci powodowana jest dołączaniem abonentów) oraz zamknięcie ruchu lokalnego na kolejnych poziomach koncentracji.



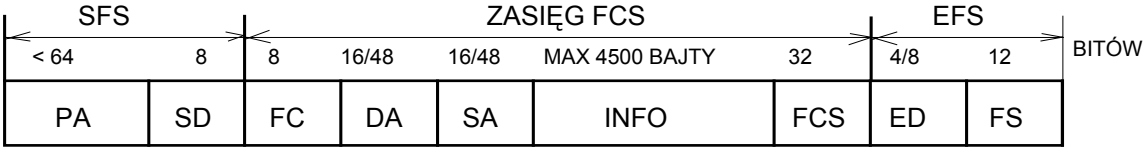
Rysunek 4.2 Sieć FDDI o strukturze podwójnej pętli z drzewami

Struktura ramek w sieci FDDI

Protokół FDDI wykazuje wiele podobieństw do protokołu Token Passing Ring. Największą jednak różnicą jest to, że w protokole FDDI przewidziano zdolność przenoszenia wielu ramek, transmitowanych w pierścieniu. Podobnie jak w protokole Token Pasing Ring w pierścieniu istnieje tylko jedna ramka tokenu. Struktury ramek przedstawiono na rysunkach 4.3. i 4.4.



Rysunek 4.3. Format ramki Token FDDI

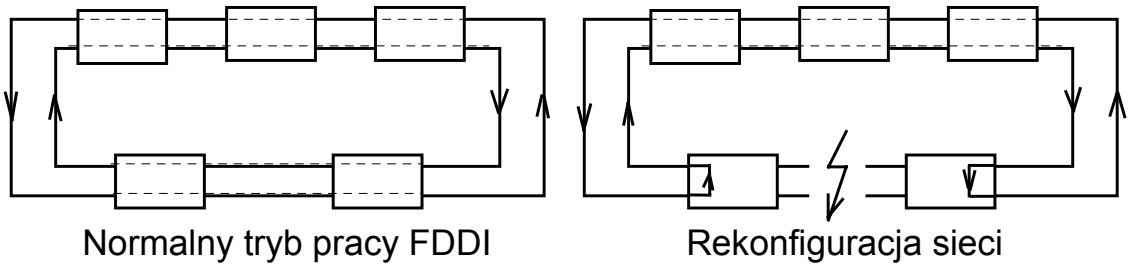


Rysunek 4.4 Format ramki FDDI

– SFS - sekwencja startowa ramki (*ang. Start of Frame Sequence*);
– PA - preambuła (*ang. Preamble*);
– SD - znacznik początku (*ang. Starting Delimiter*);
– FC - pole sterujące ramki (*ang. Frame Control*);
– DA - adres stacji docelowej (*ang. Destination Address*);
– SA - adres stacji źródłowej (*ang. Source Address*);
– INFO - pole danych (*ang. Information*);
– FCS - suma kontrolna ramki (*ang. Frame Check Sequence*);
– EFS - znacznik końca sekwencji ramki (*ang. End of Frame Sequence*);
– ED - znacznik końca ramki (*ang. Ending Delimiter*);
– FS - status ramki (*ang. Frame status*).

Niezawodność i bezpieczeństwo transmisji danych w sieci FDDI

W normalnych, nieawaryjnych warunkach pracy sieci dane użytkowników przesyłane są tylko jedną z pętli sieciowych - pętlą pierwotną. Druga z pętli (wtórna) jest wówczas poddawana jedynie kontroli jej stanu. Jest to oczywista nadmiarowość zasobów transmisyjnych, wykorzystywana jednak do poprawy niezawodności sieci. W przypadku, gdy w dowolnym miejscu łącza światłowodowego, pomiędzy dowolną parą węzłów pętli głównej wystąpi przerwa ciągłości medium transmisyjnego, sieć automatycznie zostanie przekonfigurowana, tak aby zachować połączenie pomiędzy wszystkimi węzłami sieci. Sytuację taką przedstawiono na rysunku 4.5.

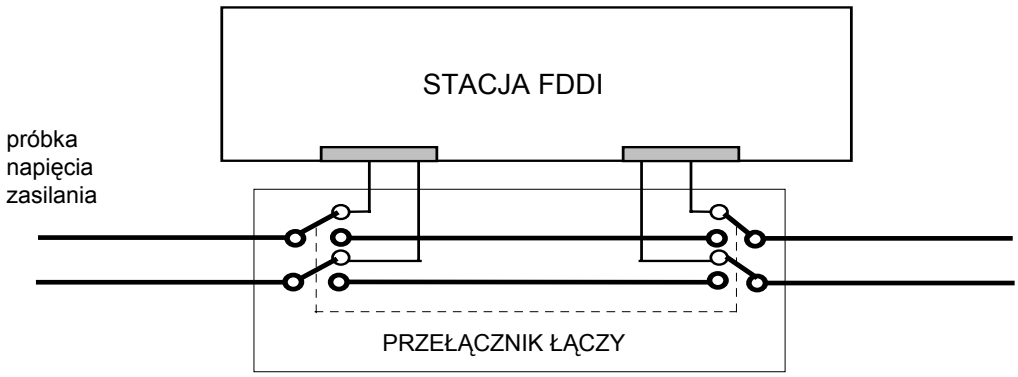


Rysunek 4.5 Przykład rekonfiguracji sieci FDDI

Sieć samoczynnie zmienia swą konfigurację również w przypadku stwierdzenia błędnej pracy jednej ze stacji. To czy utrzymana zostanie łączność z użytkownikiem dołączonym do takiej stacji zależy od charakteru powstałego uszkodzenia. Jego ocena dokonywana jest automatycznie przez procedury zarządzania pracą stacji SMT (*ang. Station Management*).

W przypadku, gdy jednocześnie w dwu miejscach przerwana zostanie ciągłość medium, sieć ulegnie podziałowi na dwie oddzielne i w pełni operacyjne podsieci. Sytuacja taka trwa do momentu usunięcia jednego z powstałych uszkodzeń. Opisane przypadki dotyczą oczywiście sytuacji, w której przerwane są obydwa włókna światłowodowe tj. pętli pierwotnej i pętli wtórnej. Jeżeli uszkodzenie dotyczy tylko jednej pętli, sieć zachowuje pełną sprawność.

Następną przyczyną mogącą pogorszyć albo wręcz uniemożliwić transmisję danych w sieci FDDI jest zanik napięcia zasilania jednej lub kilku ze stacji sieciowych. Każda ze stacji, ze względu na charakter medium transmisyjnego musi nieustannie wzmacniać i powtarzać sygnał optyczny. Zanik zasilania uniemożliwia spełnianie tego zadania. Rozwiązaniem tego problemu może być zastosowanie optoelektrycznego przełącznika łączy (przełącznika bypass). Przełącznik ten kieruje sygnał wejściowy do odbiornika stacji dopóki na jego końcówce obecna jest próbka napięcia zasilającego. Po jego zaniku przełącznik przechodzi do stanu, w którym sygnał wejściowy przekazywany jest bezpośrednio na końcówkę łącza poprzednio dołączonego do nadajnika stacji, tym samym stacja FDDI nie bierze udziału w retransmisji sygnału wejściowego. Zasada pracy pokazana została na rysunku 4.6.



Rysunek 4.6 Zasada działania przełącznika łączy

Ze względu na fakt, że każda stacja FDDI pełni rolę retransmitera i wzmacniacza sygnału, należy tak dobrać odległości między stacjami oraz typ medium transmisyjnego (światłowodu) w sieci FDDI, by poziom sygnału po odłączeniu dowolnej stacji zapewniał poprawną pracę reszty sieci. Stosowanie przełączników łączy typu bypass wymaga starannego przeanalizowania prawdopodobieństwa zestawienia ciągu zwartych przełącznikami odcinków światłowodu o długości większej od maksymalnej, dopuszczalnej odległości pomiędzy sąsiednimi stacjami. Jeśli prawdopodobieństwo takie byłoby zbyt niskie, należy rozważyć zastosowanie światłowodu lepszej jakości (światłowodu jednomodowego) pozwalającego zwiększyć odległość pomiędzy sąsiednimi, czynnymi stacjami, albo też należy wyposażyć stacje w awaryjne źródła zasilania UPS.

Wszelkie nieprawidłowości w działaniu sieci, wynikające z błędów w funkcjonowaniu stacji dołączonych do sieci poprzez koncentratory, są samoczynnie wykrywane i usuwane w obrębie samych koncentratorów. Procedury zarządzające pracą stacji tego typu automatycznie odetną dostęp do tej części sieci, w której stwierdzą obecność stacji zakłócających pracę pozostałych użytkowników. Ponowne przyłączenie do sieci nastąpi po przeprowadzeniu zestawu testów przez wszystkie dotknięte ograniczeniem dostępu do medium stacje. Żądanie odcięcia dostępu dla określonej części sieci danego węzła może wystosować operator sieci z centrum zarządzania siecią, jeśli stwierdzi, iż zachowanie któregoś z użytkowników zagraża bezpieczeństwu sieci lub grodzi w poufność danych transmitowanych poprzez sieć. Protokół FDDI uniemożliwia podłączenie stacji nielegalnych do sieci.

Tryby realizacji usług w sieci FDDI

Tryb asynchroniczny

Podstawową usługą sieci FDDI jest transmisja danych od użytkowników realizowane w trybie asynchronicznym. Protokół MAC zapewnia podział czasu dostępu do medium pomiędzy wszystkich użytkowników. W trybie asynchronicznym wysyłane są wszystkie dane nie wymagające ścisłych zależności czasowych między chwilą wysłania informacji i jej odbiorem. Typowym przykładem może być w tym przypadku transmisja plików lub poczta elektroniczna. W trybie tym istnieje pewne różne od zera prawdopodobieństwo, że stacja FDDI odrzuci nasze dane (np. przy przepełnieniu buforów) i konieczne będzie podjęcie kolejnych prób dostępu do sieci. Użytkownik sieci posiadający odpowiednie uprawnienie może zapewnić sobie nieograniczony dostęp do przepływności realizowanej w trybie asynchronicznym poprzez zastrzeżenie tokenu. Transmisja z tokenem zastrzeżonym kontrolowana jest przez procedury zarządzające pracą stacji i sieci. Nie należy jednak tej możliwości nadużywać ze

względu na całkowitą utratę dostępu do usług asynchronicznych pozostałych użytkowników. Wielu producentów nie implementuje tego typu usług ze względu na złożoność procedur nim sterujących.

Tryb synchroniczny

Transmisja synchroniczna dotyczy wszystkich źródeł danych o ścisłych zależnościach czasowych, jak transmisja mowy, dźwięku, wizji, telesterowania itp. Kombinacja transmisji asynchronicznej z synchroniczną umożliwia obsługę przez FDDI aplikacji sieciowych o naturze multimedialnej. Z ciekawszych propozycji wybranych z ofert producentów sprzętu FDDI należy wymienić telekonferencję i zdalny nadzór mienia. Nadzór mienia poprzez sieć FDDI można realizować poprzez rozmieszczenie kamer telewizyjnych w punktach chronionych. Obraz przekazywany jest poprzez sieć do określonego miejsca. Sieć FDDI zdolna jest przenieść jednocześnie do 20 skompresowanych sygnałów wizji, ale do sieci można dołączyć dowolną liczbę kamer, a wybór aktualnie przekazujących obraz do centrum dozoru należy do obsługi sterującej kamerami poprzez kanał telesterowania. Wyposażenie niezbędne do realizacji konkretnych usług prezentowane jest przez producentów sprzętu teleinformacyjnego.

Modyfikacja sieci FDDI - FDDI - II

Funkcjonalnym rozszerzeniem sieci FDDI jest sieć FDDI-II. Wzbogacona została ona o możliwość transmisji danych w trybie komutacji kanałów, przy zachowaniu łącznej szybkości transmisji 100 Mb/s. Zostało zachowane ograniczenie na maksymalną ilość stacji w sieci i jej rozmiary.

FDDI-II jest w rzeczywistości zupełnie odmienną siecią w stosunku do FDDI. FDDI-II nie jest siecią z krążącym w sieci tokenem jak w FDDI, a siecią z komutacją szczelin czasowych - niemożliwa jest, zatem współpraca urządzeń sieciowych pracujących w standardzie FDDI z urządzeniami sieci FDDI-II. Pomimo upływu czasu sprzęt dla sieci FDDI-II nie pojawił się w komercyjnej ofercie producentów, powodem jest rozwój innych sieci z integracją usług.

Modyfikacja sieci FDDI - FFOL (*ang. FDDI Follow - On Lan*)

FFOL jest aktualnie opracowywanym standardem sieciowym, mającym stanowić następną generację światłowodowych sieci komputerowych. Prace nad FFOL prowadzone są w ramach tego samego komitetu ANSI, który opracował FDDI, FDDI-II. FFOL zapowiadany jest jako sieć o charakterze lokalnym LAN (podobnie jak to miało miejsce dla FDDI). Należy jednak spodziewać się, że w chwili pojawienia się na rynku FFOL zacznie ona spełniać rolą sieci bazowej dla wolniejszych sieci lokalnych.

Po trzech latach prac komitetu dostępne są jedynie wstępne założenia i propozycje uzgodnione z największymi producentami sprzętu teleinformatycznego.

FFOL ma charakteryzować się następującymi cechami:

- różnorodnością usług, w tym transmisją asynchroniczną i synchroniczną w pasmie 6.144 Mb/s;
- zgodnością szybkości transmisji ze standardami sieci synchronicznych;
- możliwością współpracy z sieciami ATM;
- możliwością wykorzystania okablowania charakterystycznego dla FDDI.

Tempo postępu prac nad FFOL, konkurencja ze strony innych rozwiązań oraz brak powodzenia FDDI - II budzą obawy, że FFOL stanie się kolejnym opracowanym przez komitet normalizacyjny standardem, charakteryzującym się brakiem zainteresowania ze strony producentów.

4.2 DQDB

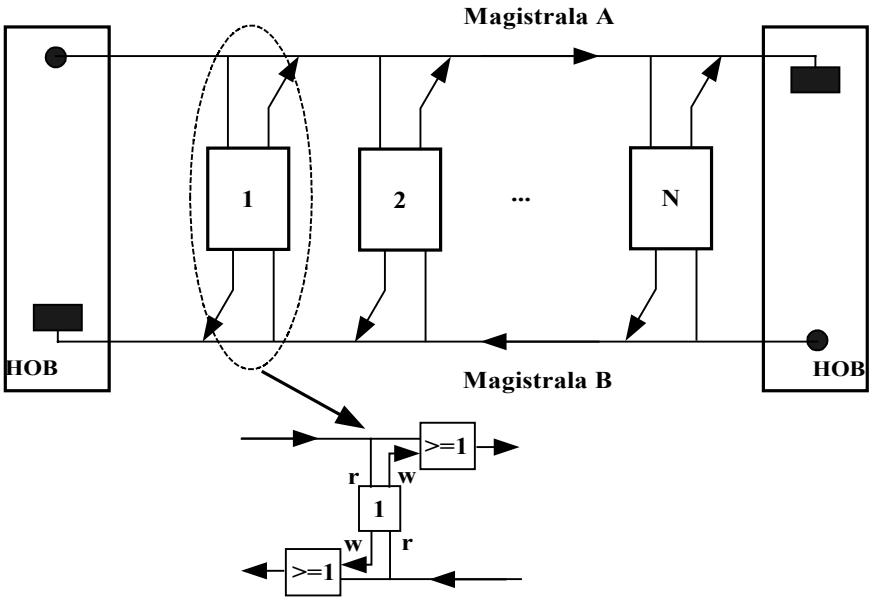
Topologia sieci

Standard IEEE 802.6 DQDB (*ang. Distributed Queue Dual Bus*) stał się dominującym standardem w dziedzinie konstruowania szybkich sieci miejskich, które mają zdolność do integracji usług. Został on także przyjęty przez ETSI jako podstawa do konstruowania europejskich sieci MAN.

Sieć DQDB oparta jest na dwóch magistralach, w których transmisja odbywa się w dwóch przeciwnych kierunkach. Jej struktura przedstawiona jest na rysunku 4.7. Jak można zauważyć sieć taka gwarantuje połączenie między dowolną parą węzłów w pełnym dupleksie.

Stacja początkowa (HOB) generuje ciąg sygnałów synchronizacji na magistrali, które wyznaczają ramki o długości 125μs. Każda ramka jest z kolei podzielona na pewną liczbę szczelin. Stacja końcowa (HOB) stanowi zakończenie magistrali - usuwa ona wszystkie napływające szczeliny, a także generuje ramki z taką samą szybkością (lecz nie koniecznie fazą) na drugiej magistrali.

Węzły są dołączone do magistrali za pomocą urządzeń umożliwiających odczytywanie danych z magistrali jak i wprowadzanie do niej danych do przesłania. Wpisywanie danych na magistralę odbywa się przez bramkę OR, na której wejścia podawane są bity danych przepływające przez magistralę oraz dane pochodzące z danego węzła. Urządzenie odbiorcze danych z magistrali dołączone jest do magistrali przed urządzeniem do zapisu danych do magistrali. Zatem odczyt następuje wprost i dane te w żaden sposób nie są zakłócane przez dane, które dany węzeł wysyła. Należy także zauważyć, że dane przepływają poza węzłami, zatem awaria węzłów względnie ich usunięcie nie powoduje przerwy w pracy sieci. Awarię pracy sieci może wywołać uszkodzenie magistrali lub niekontrolowany wypływ danych z jakiegoś węzła. Uszkodzenie magistrali wymaga rekonfiguracji sieci, natomiast niekontrolowany wypływ danych może być rozpoznany przy użyciu procedur wykrywających błędy i rozwiązany przez separacją uszkodzonych układów.



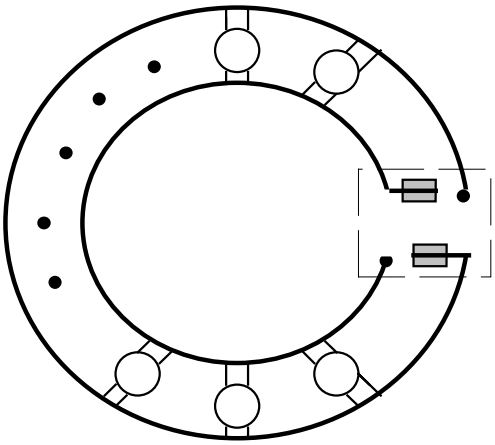
Rysunek 4.7 Struktura sieci DQDB

Najczęściej spotykaną strukturą sieci DQDB jest struktura pierścienia (rysunek 4.8), zastosowanie tego typu modyfikacji ma dwa cele:

- generator impulsów wyznaczający ciąg ramek czasowych może być ten sam dla obu magistral;
- w przypadku fizycznego przerwania magistrali lub awarii można dokonać prostej rekonfiguracji systemu, omijając uszkodzone miejsce.

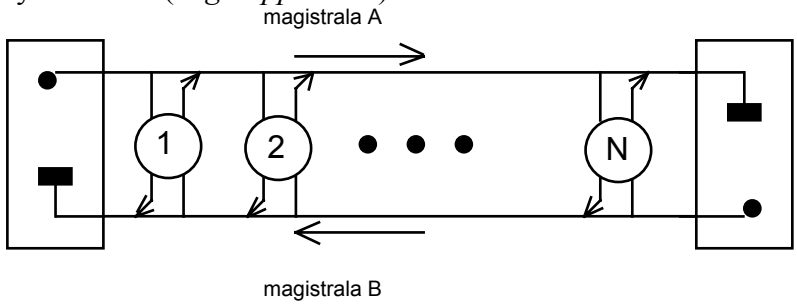
Sieć DQDB może znajdować się w trzech różnych konfiguracjach:

- pierścienia (*ang. normal*).



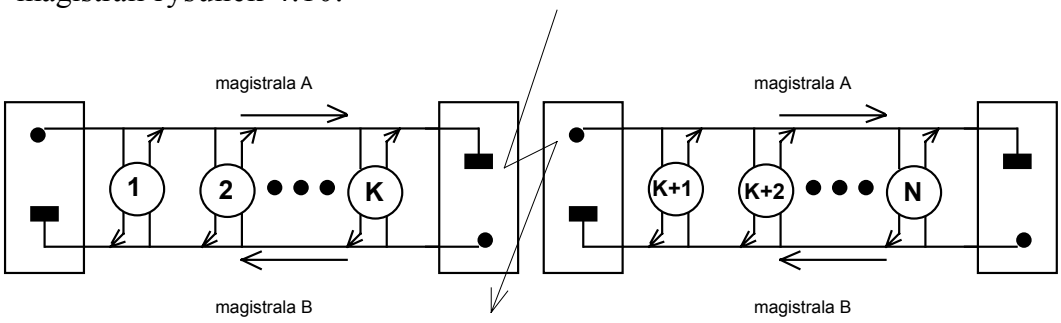
Rysunek 4.8 Sieć DQDB o strukturze pierścienia

- magistrali, rysunek 4.9 (*ang. lopped bus*).



Rysunek 4.9 Sieć o strukturze magistrali

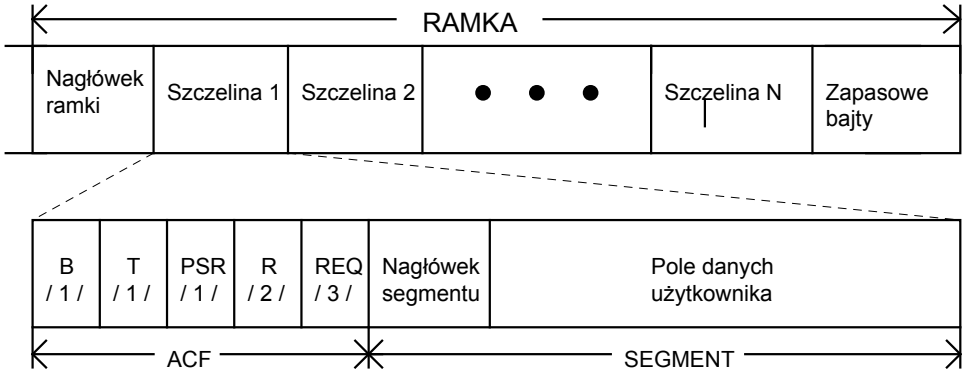
- wysp (*ang. islands*), w przypadku awarii sieć rozpada się na kilka sieci o strukturze magistrali rysunek 4.10.



Rysunek 4.10 Sieć o strukturze wysp

Struktura ramki, mechanizm rezerwacji szczelin

Wymiana informacji w sieci DQDB odbywa się przy pomocy ramek (*ang. frames*). Struktura ramki została przedstawiona na rysunku 4.11.



Rysunek 4.11 Struktura ramki w sieci DQDB

ACF - pole sterujące, wykorzystywane do sterowania dostępem do szczelin (*ang. Access Control Field*):

- B - bit zajętości (*ang. busy*), B = 0 - szczelina wolna; B = 1 - szczelina zajęta;
- T - bit typu szczeliny (*ang. SI Type*), bit wskazujący typ szczeliny T = 1 - szczelina dla usługi synchronicznej, T = 0 - szczelina dla usługi asynchronicznej;
- PSR - bit wskazujący, czy poprzednia szczelina została odebrana, czy też nie (*ang. Previous Slot Received*);
- R - 2 bity nie wykorzystane, zarezerwowane do przyszłego wykorzystania (*ang. Reserved*);
- REQ - 3 bity rezerwujące szczeliny, wskazują, że stacja oczekuje na przyznanie szczeliny; na podstawie tych bitów rozpoznawany jest także priorytet informacji oczekującej do nadania (*ang. Request*).

Długość ramki wynosi 125 μs ze względu na dopasowanie jej do obowiązujących standardów telefonii cyfrowej. Ramka podzielona jest na pewną liczbę szczelin, z których każda oprócz bitów nadmiarowych ma dostępne 48 oktety przeznaczone do transmisji. Każda szczelina może być przeznaczona dla innego rodzaju transmisji:

- synchronicznej, dla usług realizowanych w trybie komutacji kanałów (np. transmisja mowy, transmisja obrazów ruchomych itp.); wówczas szczeliny są określone jako PA (*ang. PreArbitrated*).
- asynchronicznej, dla usług realizowanych w trybie komutacji pakietów (np. transmisja danych) wówczas szczeliny są określane jako QA (*ang. Queued Arbitrated*).

Szczeliny typu PA są przydzielane przez stacje HOB (początkowe i końcowe), co jest wskazywane przez odpowiednie ustawienie bitów B i T, które znajdują się w polu ACF. W przypadku transmisji synchronicznej jeden oktet umieszczany w szczelinie jest równoważny kanałowi o przepustowości 64 kb/s. Umieszczając więcej oktetów w szczelinie można otrzymać kanał o wyższej przepustowości.

W przypadku transmisji asynchronicznej, szczeliny przydzielane są na żądanie, umieszczane są w nich fragmenty pakietów tzw. segmenty. Dostęp do poszczególnych szczelin jest uzyskiwany w oparciu o protokół DQDB.

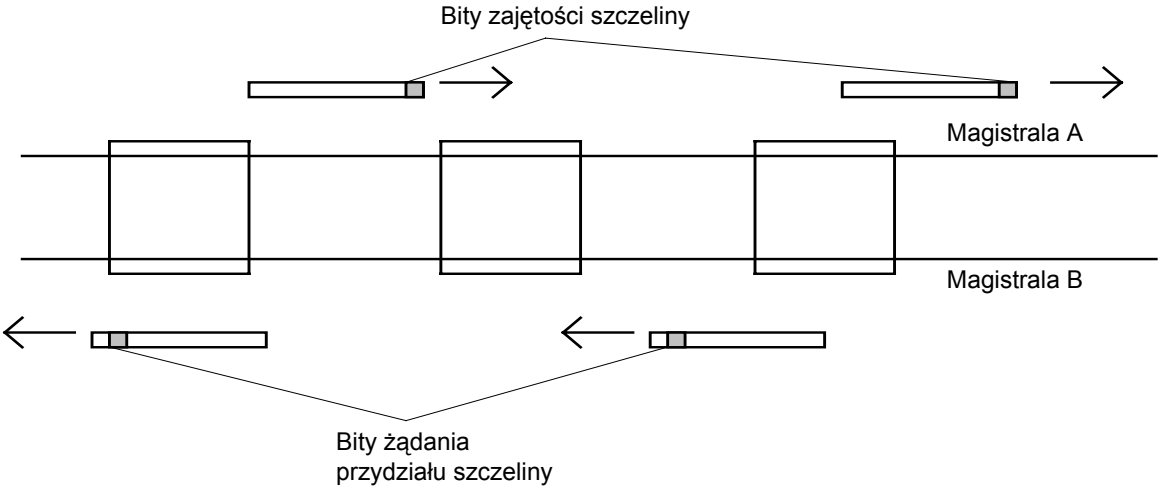
Struktura ramki w sieci DQDB (rysunek 41) jest podobna do struktury ramki w sieci B-ISDN. Przyjęta struktura ramki umożliwia łatwą konwersję ramek między siecią MAN - DQDB i rozległą siecią B-ISDN.

Protokół dostępu do medium transmisyjnego (protokół DQDB)

W celu jasnego zaprezentowania protokołu dostępu DQDB przedstawiona zostanie wersja uproszczona (tj. bez klas priorytetów). Jak dotąd nie rozwiązano wszystkich zagadnień związanych z transmisją segmentów o różnych priorytetach, np. "sprawiedliwy" podział przepływności w przypadku przeciążenia systemu. W pierwszych implementacjach sieci DQDB zakłada się, że wszystkie segmenty mają jednakowy priorytet.

W wersji uproszczonej protokół wykorzystuje bity sterujące umieszczone w nagłówku szczeliny (pole ACF): bit zajętości (B) i bity z żądaniem (REQ). Bity REQ służą do wskazania żądania przyznania szczeliny przez stację HOB, w której to szczelinie zostanie umieszczony segment danych (odbywa się to w sposób niezależny dla obu magistral). Zadaniem bitu zajętości jest wskazanie innym stacjom sieci, że szczelina jest już zarezerwowana do transmisji segmentu danych, a zatem, że jest ona niedostępna dla innych użytkowników.

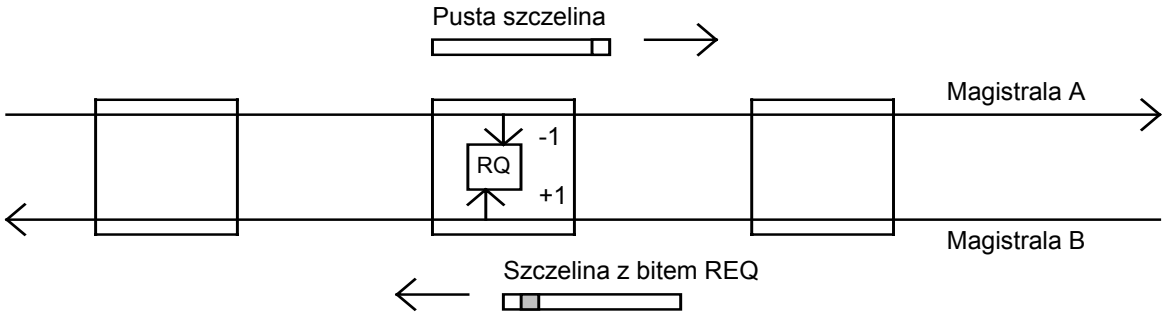
Rozważone zostanie działanie protokołu w przypadku, gdy segmenty są transmitowane w ramkach magistralą A, co przedstawione jest na rysunku 4.12. Transmisja segmentów magistralą B jest w pełni symetryczna do magistrali A.



Rysunek 4.12 Zasada działanie protokołu DQDB

W przypadku, gdy dany węzeł chce przesłać segment magistralą A, to wówczas będzie się on starał nadać bity REQ magistralą B. Bity te docierają do wszystkich węzłów leżących na magistrali A w kierunku przeciwnym do kierunku transmisji, poczynając od węzła, który nadał bit REQ. Bity REQ sygnalizują węzłom, że w kolejce do transmisji (na magistrali A) został umieszczony segment.

W sytuacji, gdy węzeł nie ma segmentu do nadania, to śledzi on na bieżąco liczbę segmentów umieszczonych w kolejce a pochodzących z węzłów położonych w kierunku transmisji na magistrali A. Realizowane jest to poprzez zliczanie kolejnych żądań, które transmitowane są magistralą B. Każde odebrane bity REQ powodują zwiększenie stanu licznika RQ (znajdującego się w każdym węźle sieci) o jeden (rysunek 4.13).

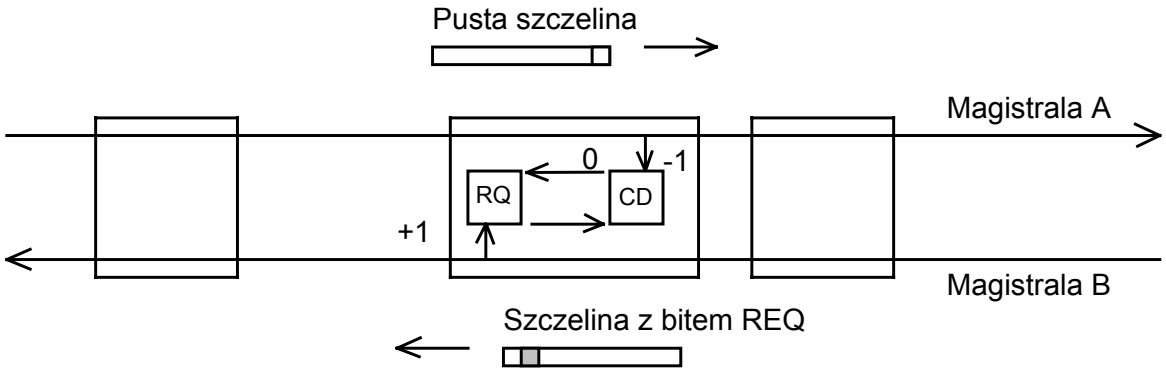


Rysunek 4.13 Ilustracja pracy licznika RQ

Natomiast każda transmitowana pusta ramka na magistrali A powoduje zmniejszenie stanu licznika RQ o jeden. Dzieje się to, dlatego, że z prawdopodobieństwem równym jedności przepływająca pusta ramka zostanie wykorzystana przez któryś z węzłów. Jak łatwo można zauważyć stan licznika w każdym węźle odzwierciedla precyzyjnie stan kolejki segmentów oczekujących na nadanie przez węzły leżące w kierunku transmisji na magistrali A.

Nieco inaczej wygląda sytuacja, gdy dany węzeł ma do nadania segment. Wówczas po nadaniu bitów REQ uruchamiany jest w tym węźle drugi licznik CD, w którym za stan początkowy przyjmuje się aktualny stan licznika RQ, a następnie licznik RQ jest zerowany. To w konsekwencji powoduje, że stan licznika CD jest równy liczbie segmentów oczekujących w węzłach leżących w kierunku transmisji na magistrali A. Stan licznika CD jest zmniejszany o jeden, gdy magistralą A przepływa pusta szczelina. Dany węzeł może nadać swój segment, gdy stan licznika CD osiągnie wartość zero. Segment może być nadany w pierwszej pustej szczelinie transmitowanej magistralą A.

W czasie, gdy węzeł oczekuje na uzyskanie dostępu do magistrali, po której nada swój segment, każdy nowy bit REQ odebrany z magistrali B powoduje zwiększenie stanu licznika RQ o jeden. Zatem stan ten w dalszym ciągu odzwierciedla liczbę segmentów oczekujących na transmisję w węzłach leżących w kierunku transmisji na magistrali A. Pracę liczników CD i RQ przedstawiono na rysunek 4.14.



Rysunek 4.14 Ilustracja pracy liczników CD i REQ

Cechą charakterystyczną standardowej wersji DQDB jest to, że pojedyncza szczelina może być wykorzystywana jedynie raz, gdy transmitowana jest wzdłuż magistrali. Prowadzone są prace badawcze nad umożliwieniem wielokrotnego wykorzystania pojedynczej szczeliny, co zwiększyłoby przepustowość sieci. Zaproponowano między innymi wprowadzenie specjalnych węzłów posiadających

zdolność zwalniania szczelin, z których zostały wcześniej odczytane segmenty. Węzły takie nazwano węzłami kasującymi. Aktualny standard sieci DQDB przewiduje wykorzystanie bitu PSR (z pola ACF) do sygnalizacji czy segment znajdujący się w szczelinie dotarł do swojego adresata. Jeśli węzeł rozpozna, że segment w danej szczelinie jest adresowany do niego, to jest on zobowiązany do ustawienia bitu PSR w następnej szczelinie. Każdy węzeł kasujący opóźnia ciąg bitów transmitowanych magistralami o jedną szczelinę i wydłuża czas konieczny do stwierdzenia czy w następnej szczelinie bit PSR jest ustawiony. Jeśli tak to bit ten jest zerowany i jednocześnie zwalniana jest szczelina poprzez wyzerowanie jej zawartości. Zastosowanie węzłów kasujących nie wymaga żadnych zmian w działaniu normalnych węzłów, które w zależności od implementacji mogą być w sposób pasywny lub aktywny podłączone do magistral. Wprowadzenie węzłów kasujących ma dwie zasadnicze zalety:

- zwiększenie przepustowości sieci, wprowadzenie K węzłów w skrajnym przypadku może spowodować (K+1) krotny wzrost maksymalnej przepustowości;
- węzły kasujące mogą izolować od reszty sieci grupy użytkowników o wzajemnych interesach lub którzy nie życzą sobie aby np. tajne informacje krążyły po całej sieci.

Wpływ parametrów fizycznych sieci na jakość usług

Z działania protokołu DQDB wynika, że gdyby czas propagacji sygnału w magistrali był nieskończenie mały i równocześnie szybkość transmisji była nieskończenie duża, to segmenty pochodzące od różnych węzłów obsługiwane byłyby w myśl reguły FIFO, tj. obsługiwane zgodnie z kolejnością, z jaką pojawiały się w węzłach. Niestety, w praktyce czas propagacji w światłowodzie wynosi około 5μs/km a szybkości transmisji są rzędu kilkudziesięciu do kilkuset Mbit/s.

W praktyce istnieje jeszcze jeden bardzo istotny problem. Rozważając zachowanie się systemu możemy zauważyć, że węzły leżące bliżej czoła magistrali X (bliżej węzła HOB) mogą znacznie częściej uzyskiwać dostęp do wolnych szczelin transmitowanych magistralą X, niż węzły leżące przy końcu magistrali X. Spowodowane to jest faktem, że np. węzeł leżący przy końcu magistrali może 'nie wiedzieć', że po tej magistrali przepływa żądanie wystosowane przez węzeł leżący na początku magistrali X. Jest rzeczą oczywistą, że ten efekt, który powoduje niesprawiedliwy dostęp do magistrali X, potęguje się wraz ze wzrostem długości magistral.

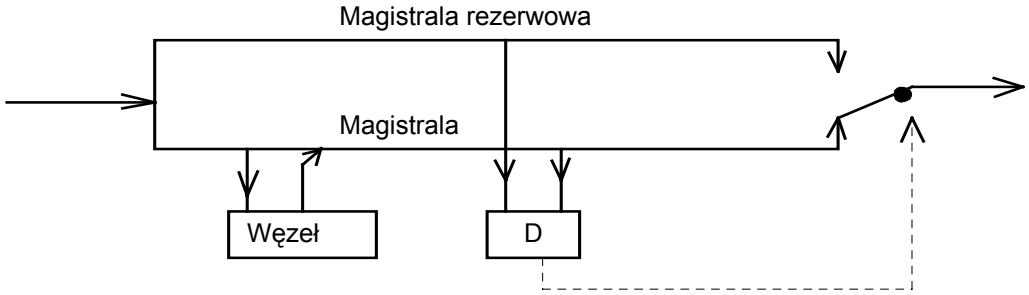
Problem równych szans dostępu do magistrali, który uzyskują węzły, niezależnie od ich położenia w sieci w przypadku przeciążeń, został rozwiązany przez wprowadzenie do standardu DQDB tzw. mechanizmu BWB (*ang. Bandwidth Balancing*). Mechanizm ten polega na tym, że węzeł, który nadał M segmentów przepuszcza szczelinę przeznaczoną dla niego, nie nadając w niej segmentu. Analiza wykazuje, że jest to mechanizm ze sprzężeniem zwrotnym, który stabilizuje działanie systemu. W stanie przeciążenia wszystkie węzły otrzymują taką samą przepustowość.

Stosowanie mechanizmu BWB nie jest obowiązkowe. Wartość parametru M jest ustalana przez operatora sieci jak również on decyduje o tym czy ten mechanizm zostanie użyty.

Niezawodność sieci DQDB

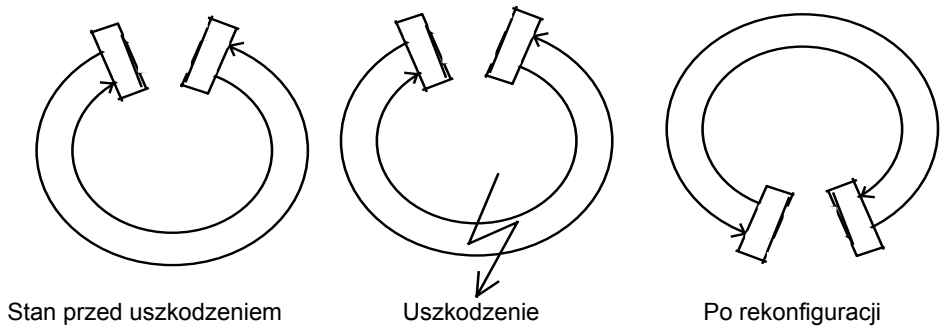
Jednym z podstawowych kryteriów, jakie musi spełniać sieć, jest jej niezawodność. Wysoka niezawodność sieci DQDB wynika z kilku faktów. Po pierwsze dane nie przepływają przez węzły, a zatem uszkodzenia pasywne w warstwie MAC nie powodują utraty zdolności transmisyjnej sieci.

Po drugie, wpisywanie informacji na magistrale odbywa się za pomocą bramki OR, zatem uszkodzenie aktywne w warstwie MAC jak i uszkodzenia na magistrali można łatwo wykryć porównując sygnały wejściowe z wyjściowymi. Wówczas uszkodzone miejsce można w prosty sposób ominąć, tak jak to przedstawiono na rysunku 4.15 (D - urządzenie wykrywające uszkodzenie). Operację taką przeprowadza się na poziomie sprzętowym i potencjalne zakłócenia są minimalne.



Rysunek 4.15 Ilustracja sposobu przeciwdziałania uszkodzeniom

W przypadkach fizycznych uszkodzeń magistrali dokonywana jest automatyczna rekonfiguracja sieci. Przedstawia to rysunek 4.16. Uszkodzona część magistrali zastępowana jest naturalną "przerwą" w sieci, podczas gdy poprzednia "przerwa" zostaje zlikwidowana.



Rysunek 4.16 Rekonfiguracja sieci w przypadku fizycznego uszkodzenia magistrali

4.3 Usługi CBDS/SMDS

Gwałtowny spadek cen na systemy przetwarzania danych w ostatnich latach doprowadził do bardzo szerokiego rozpowszechnienia tych systemów w wielu dziedzinach życia. Jednakże z drugiej strony wzrosło zapotrzebowanie na transfer bardzo dużych ilości danych w stosunkowo krótkim czasie. Typowymi zastosowaniami dla szybkiego transferu danych jest np. transfer dużych zbiorów, wymiana dokumentów, czy też przesyłanie obrazów. Wzrasta także odległość pomiędzy komunikującymi się ze sobą komputerami i niestety klasyczne sieci LAN nie są w stanie sprostać takim wymaganiom. Okazuje się także, że użytkownicy w wielu rzeczywistych systemach raczej sporadycznie mają zapotrzebowanie na transfer danych. Oznacza to, że wykorzystanie dostępnej dla użytkownika przepustowości jest niepełne. Z przesłanek tych wynika konieczność określenia usługi nowego typu, spełniającej dość ostre wymagania, i opartej na dostępnej technologii.

Usługą spełniającą wymagania stawiane przez użytkowników jest usługa CBDS zdefiniowana dla Europy i SMDS zdefiniowana dla Stanów Zjednoczonych (*ang. Connectionless Broadband Data Service/Switched Multimegabit Data Service*). CBDS i SMDS są terminami przyjętymi odpowiednio przez ETSI i Bellcore (*ang. Bell Communications Research*) dla usług szybkiego transferu danych w obszarze miejskim lub większym.

Obie usługi są w bardzo znacznym stopniu do siebie podobne. Między innymi obie stosują protokół DQDB dostępu do medium transmisyjnego. Oczekuje się, że w przyszłości dojdzie do pełnej integracji obu usług. Ze względu na podobieństwo tych usług, zostanie omówiona jedna z nich SMDS.

Usługa jest usługą publiczną opartą na technice komutacji pakietów. Zapewnia komunikację między odległymi punktami z szybkościami transmisji wynoszącymi: 1.2, 4, 10, 16, 25 i 34 Mb/s. SMDS jest przewidziana do obsługi wzrastających potrzeb na komunikację pomiędzy odległymi sieciami LAN, stacjami roboczymi, dużymi komputerami i urządzeniami peryferyjnymi. Wprowadzenie SMDS w sposób znaczący zmniejsza koszty ponoszone przez użytkowników. Usługa SMDS spełnia zapotrzebowanie użytkowników na łączenie ze sobą sieci LAN poprzez oferowanie możliwości, które dotychczas były charakterystyczne dla sieci LAN.

Obecnie w Stanach Zjednoczonych firmy telekomunikacyjne w sposób intensywny zaczynają oferować usługę SMDS. Tak, więc SMDS jest w zasadzie już rzeczywistością.

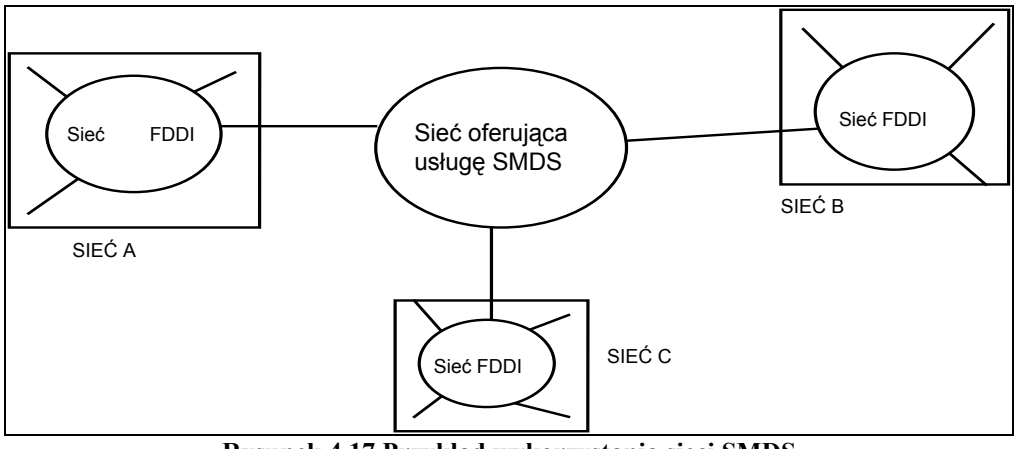
Usługa CBDS jest opisana w dokumencie ETSI91, a SMDS w serii zaleceń Bell91a-e.

Poniżej są przedstawione podstawowe charakterystyczne cechy usługi SMDS:

- jest ona podobna do usług oferowanych w sieciach LAN;
- zapewnia weryfikację adresów źródłowych;
- zapewnia kontrolę (*ang. screening*) adresów źródłowych i docelowych;
- zapewnia adresowanie grupowe;
- określa maksymalną długość pakietu;
- gwarantuje możliwość łączenia ze sobą użytkowników zarówno w skali krajowej jak i międzynarodowej.

Dostęp do usług SMDS

Każdy klient usługi SMDS ma indywidualny kanał, za pomocą którego może uzyskiwać dostęp do sieci SMDS, tak jak to przedstawiono na rysunku 4.17.



Rysunek 4.17 Przykład wykorzystania sieci SMDS

Każdy klient ma dostęp do pełnej przepustowości tego kanału. Każdy adres źródłowy jest sprawdzany czy jest on adresem, który jest dopuszczalny dla danego kanału dostępowego. Zapewnia to pełną poufność i bezpieczeństwo transmitowanych danych poprzez ten kanał.

Dostęp do usługi oparty jest na bezpołączeniowym protokole leżącym w warstwie MAC, który został opisany w standardzie IEEE 802.6. Usługa SMDS została zaprojektowana w taki sposób, aby urządzenia komunikacyjne klienta, takie jak np. router lub karta wewnętrzna stacji roboczej, mogły zapewnić dostęp do sieci oferującej usługę SMDS.

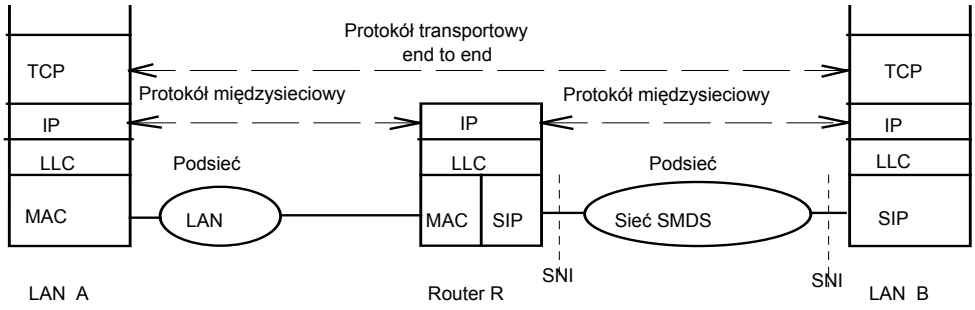
Architektura SMDS

Sieć SMDS stanowi podsieć, jeśli rozważona zostanie pełna architektura sieciowa klienta. SMDS obejmuje funkcje na dwóch najniższych poziomach w modelu warstwowym OSI/ISO i zapewnia usługę na poziomie MAC. Przykładowa architektura została przedstawiona na rysunku 4.18. (gdzie SMDS jest częścią sieci TCP/IP łączącą sieci LAN ze sobą).

Protokół SIP

Sprzęt abonenta może być dołączony bezpośrednio do sieci SMDS, przy czym zastosowany zostaje protokół SIP (*ang. SMDS Interface Protocol*). SIP oparty jest na bezpołączeniowym protokole MAC opisanym w zaleceniu IEEE90. Jednostki danych warstwy trzeciej L3_PU (*ang. Level 3 Protocol Data Unit*) zawierają jednostki danych SDU (*ang. SMDS Service Data Units*). Jednostki danych protokołu warstwy trzeciej są dzielone na jednostki danych odpowiednio dostosowane do opisu warstwy drugiej. Jednostka danych SIP L3_PDU przedstawiona została na rysunku 4.19.

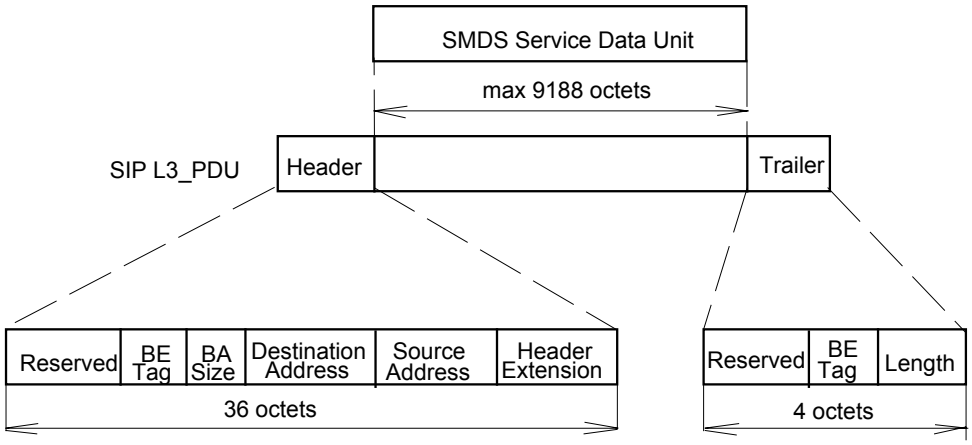
Adres źródła i adres przeznaczenia składają się z 64 bitów i są przenoszone w nagłówku każdej jednostki L3_PDU. Cztery najbardziej znaczące bity pola adresowego służą do wskazania, czy jest to adres indywidualny czy grupowy, pozostałe bity służą do przenoszenia 60 bitowego adresu SMDS, który podlega administracji sieci. Adres ten jest zapisany w kodzie BCD (*ang. Binary Coded Decimal*) i imituje format używany dla numerów telefonicznych.



TCP - Transmission Control Protocol
IP - Internet Protocol
SIP - SMDS Interface Protocol
SNI - Subscriber Network Interface
LLC - Link Level Control
MAC - Medium Access Control

Rysunek 4.18 Rola SMDS w łączeniu ze sobą abonentów sieci

Pola BE Tag (*ang. Beginning End*), rozmiar bufora (*ang. Buffer Allocation Size*) i pole rozmiar (*ang. Length*), znajdujące się w nagłówku i zakończeniu jednostki, są używane przez procedury sterujące stacji nadawczych i odbiorczych. Pole rozszerzenie nagłówka (*ang. header extension*) wykorzystywane jest przy wyborze systemu transmisyjnego i przenoszone jest przez sieć SMDS niezmienione.



Rysunek 4.19 Jednostka SIP L3_PDU

Jednostka danych w warstwie drugiej (L2_PDU) odpowiada jednostce Derived MAC PDU określonej w standardzie IEEE90. Warstwa druga SIP odpowiedzialna jest za proces segmentacji jednostek L3_PDU o różnej długości na szczeliny o stałej długości. Jest on także odpowiedzialny za wykrywanie błędów poprzez zastosowanie kodu cyklicznego o wielomianie generującym 10 stopnia. Dziesięć bitów kodu nadmiarowego umieszczanych jest na końcu jednostki L2_PDU.

Warstwa pierwsza protokołu odpowiedzialna jest za dopasowanie fizycznego interfejsu do systemu transmisyjnego.

SMDS pozwala na transfer pakietów o długości nie większej od 9188 oktetów. To oczywiście przekracza maksymalne rozmiary pakietów, jakie dopuszczalne są w sieciach zgodnych ze standardami 802.X oraz FDDI (max. rozmiar pakietu 4500 oktetów). Wybór tak dużego rozmiaru pakietu podyktowany był chęcią ograniczenia procesu segmentacji przesyłanej informacji.

Każdemu interfejsowi (pomiędzy abonentem i siecią SMDS) SNI przypisany jest przynajmniej jeden adres. Adresy takie tworzone są zgodnie z zaleceniem E.164 CCITT i oparte na strukturze 15 cyfrowej. Indywidualne adresy (np. sieciowe Ethernet) użytkownika poza interfejsem SNI nie są widoczne dla sieci SMDS. O ile nie są wprowadzone ograniczenia na adresy (jak np. w prywatnych sieciach wirtualnych), to każdy abonent sieci SMDS może komunikować się z innym poprzez właściwe adresy. Jest to bardzo istotna cecha SMDS, ponieważ pozwala na komunikację ze sobą wszystkich abonentów sieci.

Usługi SMDS

Jedną z funkcji dostępowych SMDS jest kontrola (*ang. screening*) adresów źródłowych i docelowych pakietów. Polega ona na sprawdzaniu adresów, czy są one dozwolone czy też zabronione. Status adresu ustalany jest podczas podłączania abonenta do sieci. Funkcja ta umożliwia tworzenie logicznych sieci prywatnych.

Pakiety, które nie przejdą pomyślnie kontroli adresu są odrzucane. Każdy klient może zdecydować, który z ogólnie dostępnych adresów może być przez niego akceptowany.

Usługa SMDS oferuje abonentom różne przepływności:

- 1.2 Mb/s na łączu dostępowym o przepływności 1.5 Mb/s;
- 4, 10, 16, 34 Mb/s na łączu dostępowym o przepływności 45 Mb/s.

W przypadku łącza 45 Mb/s niższe szybkości reprezentują maksymalną szybkość transferu danych w przypadku nieprzerwanego nadawania danych. Natomiast w przypadku transferu sporadycznego możliwa jest szybkość do 45 Mb/s. Zastosowanie klas dostępu pozwala na efektywne wykorzystanie zarówno sprzętu należącego do abonenta jak i znajdującego się w obrębie sieci. Klasy dostępu 4, 10 i 16 Mb/s są klasami najbardziej odpowiednimi dla szeroko rozpowszechnionych sieci LAN ze względu na dopasowanie szybkości, z jaką są w nich transmitowane dane.

Zakłada się, że SMDS będzie nieprzerwanie dostępna dla abonentów, założone prawdopodobieństwo dostępności SMDS wynosi p=0.999, a zatem jest wyższe niż w sieciach lokalnych. Taka wysoka dostępność usług stanowi, że sieć SMDS jest atrakcyjna dla swych abonentów. Przesłanie danych między parą SNI (np. sieciami lokalnymi) jest praktycznie niewidoczne dla abonentów.

W sieci SMDS przewidziano, że pakiety, które zawierają błędy, zostają odrzucane. Błąd rozumiany jest tutaj w szerokim sensie i może dotyczyć długości pakietu, przekłamanych bitów wewnątrz pakietu czy też błędów wynikających z nieprawidłowego działania protokołów. Zadaniem sieci jest transfer pakietów, które wydają się być bez błędów, pomiędzy punktami końcowymi znajdującymi się w obrębie abonenta. Zatem ostateczna kontrola dokonywana jest przez urządzenia abonenta.

Aby zapewnić łatwą integrację SMDS z istniejącym telekomunikacyjnym środowiskiem abonenta określono tzw. SMDS CNM (*ang. Customer Network Management*). Wśród wielu możliwości, jakie oferuje CNM można wymienić zdolność do modyfikacji i wyszukiwania informacji o abonentach sieci, czy też uzyskiwania informacji o zachowaniu się sieci (np. intensywności ruchu interfejsu SNI). CNM wykorzystuje szeroko akceptowany protokół SNMP (*ang. Simple Network Management Protocol).*

5 Sieci rozległe

5.1 X.25

Fizyczny interfejs pomiędzy DTE i PSPDN (*ang. Packet Switched Public Data Network*) definiowany jest w zaleceniu X.21, stanowi on najniższą warstwę protokołu X.25. Warstwa łącza organizowana jest przez wersję protokołu HDLC pod nazwą LAPB (*ang. Link Access Procedure Version B*). Protokół LAPB pozwala na wolną od błędów transmisję pakietów w warstwie łącza danych (świadczącej usługi warstwie pakietowej) pomiędzy DTE i DCE.

Warstwa pakietowa-sieciowa skoncentrowana jest na niezawodnym transferze wiadomości, warstwy transportowej, nazywanymi TPDU (*ang. Transport Protocol Data Units*) a także na multipleksacji wywołań wirtualnych w pojedynczym kanale fizycznym, będącym pod kontrolą warstwy liniowej.

Warstwa fizyczna

Interfejs fizyczny pomiędzy urządzeniem abonenckim DTE i DCE, definiowany jest w zaleceniu X.21, może być organizowany z wykorzystaniem urządzeń protekcji - DCE- modemów. Modem może pracować w trybie synchronicznym, który umożliwia pracę w pełnym dupleksie, tworząc ścieżkę pomiędzy urządzeniem DTE a PSPDN. Szybkość transmisji zależna jest od jakości i typu łącza telekomunikacyjnego, typu wykorzystanego urządzenia modemowego oraz trybu zestawienia połączenia. Zalecenie X.21 definiuje interfejs dla sieci cyfrowej, dlatego przy opracowaniu zalecenia dla istniejącej sieci analogowej, w celu odróżnienia, do nazwy dodano "bis".

Warstwa Liniowa

Warstwa ta często określana jest jako poziom drugi modelu odniesienia ISO RM. Zabezpiecza ona warstwę pakietową w niezawodną transmisję informacji (wolną od błędów i duplikacji) pomiędzy urządzeniem abonenckim DTE a siecią PSPDN. Warstwa nie ma pojęcia o kanałach logicznych, do których przynależą pakiety, jest to rozpatrywane dopiero na poziomie pakietowym. Warstwa łącza wykorzystuje procedury sterowania przepływem i sterowania operacjami wykrywania i korygowania błędów transmisj, w trakcie przesyłania pakietów w połączeniach wirtualnych. Struktura ramki, sterowanie przepływem i procedury usuwania błędów w łączu bazują na protokole HDLC. Zgodnie z modelem odniesienia dla systemów otwartych, warstwa łącza dostarcza usługi warstwie wyższej - sieciowej (pakietowej), łącznie z listą jednostek danych protokołu, które są związane ze stacjami elementarnymi (*ang. entity*).

Pomiędzy DTE i węzłem sieci pakietowej wykorzystywany jest asynchroniczny tryb transmisji, inicjowane są naprzemienne komendy i odpowiedzi na komendy. Protokół steruje przepływem ramek I (informacyjnych) przez połączenie między urządzeniami DTE i węzłem sieci PSPDN. Adresowanie stacji w warstwie łącza ma za zadanie odróżnienie stacji DTE i DCE, które jest konieczne ze względu na niesymetryczny protokół warstwy łącza.

Warstwa pakietowa

Ze względu na swoją pozycję w modelu odniesienia warstwa pakietowa jest identyfikowana z warstwą sieciową. Warstwa sieciowa jest wykorzystywana przez warstwę transportową, w celu realizacji usług przez nią dostarczanych, a w szczególności transportu jednostek warstwy transportowej TPDU.

Usługi użytkownika

Usługi warstwy sieciowej zestawiono w tabeli 5.1, zaś ich przykładowe wykorzystanie przedstawiono na rysunku 5.1.

Tabela 5.1 Usługi warstwy sieciowej i odpowiednie parametry

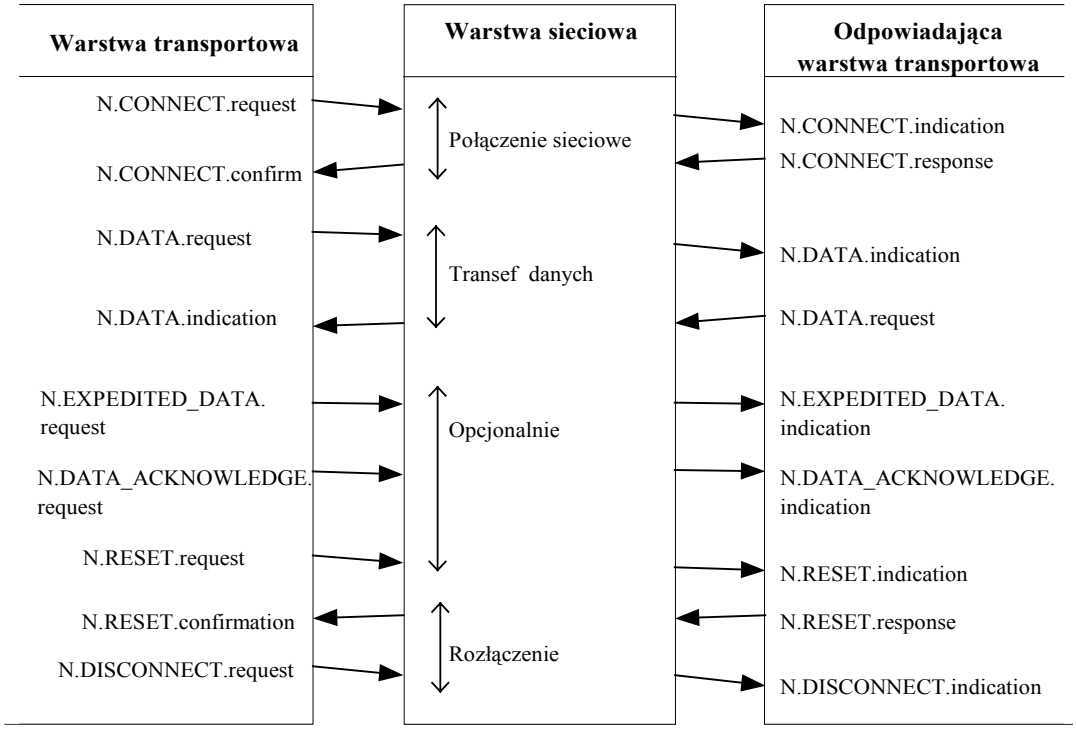
Proces elementarny, usługa	Parametry
N_CONNECT.request	Wywoływany NSAP, Wywołujący NSAP. QOS, Selekcja potwierdzenia odbioru, Selekcja nadania danych, dane NS_user
.indication	Wywoływany NSAP, Wywołujący NSAP. QOS, Selekcja potwierdzenia odbioru, Selekcja nadania danych, dane NS_user
.response	Odpowiadający (wywoływany) NSAP, QOS, Selekcja potwierdzenia odbioru, Selekcja nadania danych, dane NS_user
.confirm	Odpowiadający (wywoływany) NSAP, QOS, Selekcja potwierdzenia odbioru, Selekcja nadania danych, dane NS_user
N_DATA.request	NS_user data
.indication	NS_user data
N_DATA_ACKNOWLEDGE.	
.request	-
.indication	-
N_EXPEDITED_DATA.	
.request	NS_user data
.indication	NS_user data
N_RESET.request	Twórca,przyczyna
.indication	Twórca,przyczyna
.response	-
.confirm	-
N_DISCONNECT.request	Twórca, przyczyna, NS_user data, Odpowiadający adres
.indicator	Twórca, przyczyna, NS_user data, Odpowiadający adres

Jak można zauważyć, usługa N.EXPEDITED_DATA jest dodatkową usługą dostępną poza standardową N.DATA. Usługa umożliwia przesłanie pojedynczej informacji poza kolejnością w kanale logicznym bez przerywania normalnej wymiany informacji. Inna opcjonalna usługa N.DATA_ACKNOWLEDGE umożliwia potwierdzenie odebrania wcześniejszych pakietów, które przesyłane były w czasie realizacji usługi N.DATA. Usługa RESET umożliwia użytkownikom ponowną synchronizację sterowania ruchem pakietów w kanale logicznym. Usługa DISCONNECT realizuje rozłączenie połączenia wirtualnego. Wszystkie z funkcji elementarnych posiadają przypisane sobie parametry. Na przykład parametrami przypisanymi do usługi elementarnej N.CONNECT są: wywoływany NSAP i źródłowy NSAP. NSAP to punkt dostępu do usług warstwy N (*ang. N Service Access Point*), który jest połączeniem fizycznego adresu urządzenia i wewnętrznego (wewnątrz warstwy) identyfikatora kanału logicznego zwanego także rozszerzeniem adresu, problem ten wyjaśniony jest w punkcie dotyczącym połączenia wirtualnego.

Parametr jakość usług (*QOS - ang. Quality of Service*) zawiera dwie listy parametrów. Jedna to pożądana jakość usług, druga to jakość minimalna, która jeszcze jest akceptowana. Te parametry to: opóźnienie tranzytu, resztkowa stopa błędów, priorytet, koszt połączenia i wyspecyfikowana marszrutyzacja. Powyższe parametry są

negocjowane pomiędzy DTE a siecią w trakcie fazy transferu danych. Warstwa transportowa może posiadać kilka połączeń sieciowych, które są identyfikowane przez unikalne NSAP.

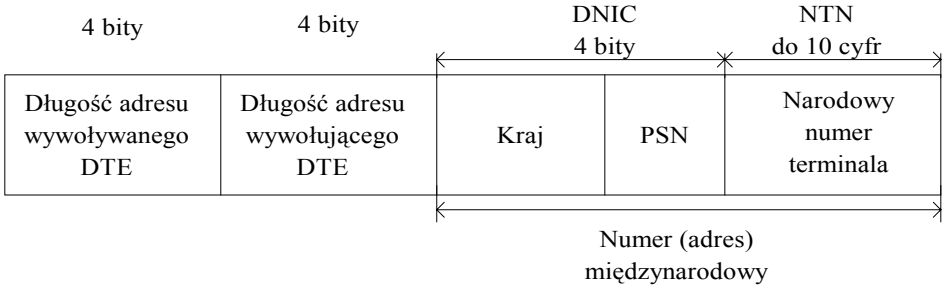
Warstwa sieciowa zabezpiecza realizację funkcji multipleksacji. Wszystkie połączenia wirtualne VC (*ang. Virtual Circuits*) i połączenia zawczasu przygotowane - stałe (*ang. Permanent VC*) - są multipleksowane w pojedynczym połączeniu sterowanym przez warstwę liniową. Sterowanie przepływem pakietów w każdym połączeniu jest oddzielnie kontrolowane przez warstwę pakietową.



Rysunek 5.1 Usługi warstwy sieciowej

Struktura adresu NSAP

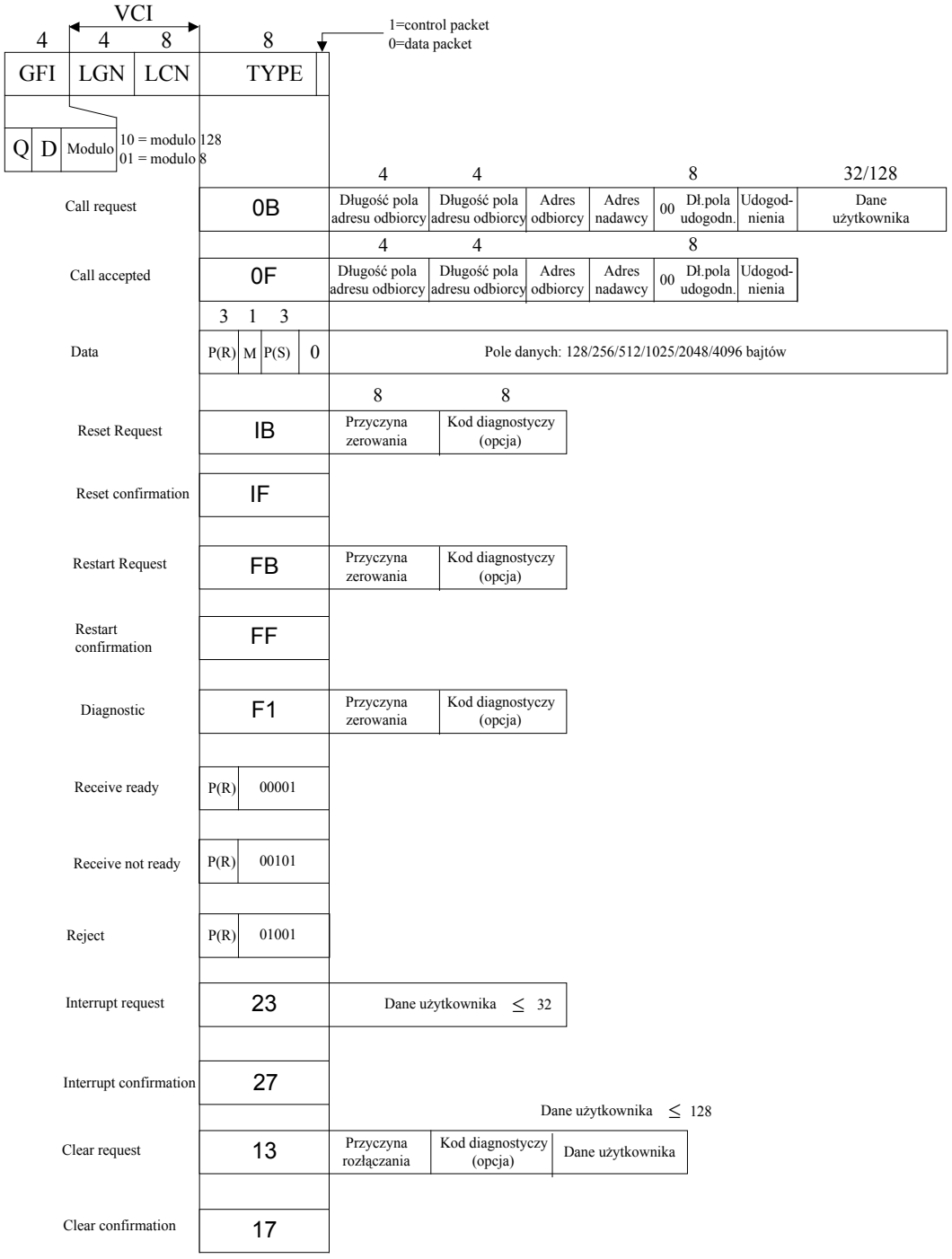
Wiele państw posiada jedną albo większą liczbę publicznych sieci komutacji pakietów (PSPDN), które są podłączone do sieci globalnej i tworzą sieć międzynarodową. W związku z tym adres dowolnej stacji DTE - NSAP musi być unikalny. Zwykle adres składa się z części identyfikującej państwo (rysunek 5.2), niektóre sieci narodowe mają numer podsieci w ramach sieci narodowej. Struktura adresu dla X.25 definiowana jest w zaleceniu X.121 CCiTT. W praktyce jednak adresacją zajmuje się ISO wraz z CCiTT.



Rysunek 5.2 Struktura adresu X.25

Typy pakietów

Pakiety są rozumiane jako jednostki danych protokołu sieciowego PPDU (*ang. packet protocol data unit*). Rodzaje i budowa pakietów przedstawione są na rysunku 5.3.



GFI - Group format identifier
LCN - Logical Channel number
P(R)Packet receiver sequence number

VCI - Virtual circuit identifier
Q - Qualifire bit
D - Delivery confirmation bit
P(S) - packet send seqence number

Rysunek 5.3 Typy i formaty pakietów w sieci pakietowej CCiTT X.25

W zależności od interfejsu, DTE/DCE albo DCE/DTE, pakiety posiadające taką samą strukturę mogą mieć inne nazwy i inne znaczenie. Na przykład struktura CALL REQUEST jest identyczna jak INCOMING CALL.

Wszystkie pakiety składają się z nagłówka, w skład którego wchodzą: identyfikator formatu grupy GFI (*ang. group format identifier*), numer logiczny grupy LGN (*ang. logical group number*) i numeru kanału logicznego LCN (*ang. logical channel number*). GFI jest 4 bitowym polem składającym się z bitu kwalifikatora Q, bitu potwierdzenia dostarczenia informacji D i dwóch bitów dodatkowych (modulo) określających zakres sekwencji liczbowych wykorzystywanych w sterowaniu przepływem (modulo 8 albo 128). Pola LGN i LCN zajmują w sumie 12 bitów, są to pola identyfikujące numer kanału logicznego VCI (*ang. virtual circuit identifier*). Następnym polem jest pole typ pakietu. W odróżnieniu od pakietów danych, wszystkie pakiety sterujące w pierwszym bajcie na pozycji najmniej znaczącego bitu mają ustawioną jedynkę.

W pakietach danych i sterowania przepływem RR, RNR, REJ (*ang. receive ready, receive not ready, reject*) umieszczane jest pole sekwencji pakietów odebranych. W pakiecie danych występuje także bit M (*ang. more*), który jest wykorzystywany w przypadku, gdy pakiet danych przechodząc przez sieć, musi zostać podzielony na mniejsze i ponownie złożony. Pole danych użytkownika może zawierać od 128 do 4096 bajtów i jest ono zależne od administratora sieci. Pakiet INTERRUPT REQUEST pozwala przesłać między użytkownikami do 32 bajtów informacji poza procedurami sterowania przepływem. Pakiet taki jest potwierdzany przez zwrotny pakiet INTERRUPT CONFIRMATION. Stany procesów DTE/DCE w protokole X.25 i wykorzystywane w tych stanach pakiety, przedstawiono w tabeli 5.2.

Tabela 5.2 Interfejs warstwy sieciowej i transportowej, międzywarstwowe funkcje elementarne

Typy pakietów (PPDU)		**Faza realizacji, stan procesu**
DTE → DCE	**DCE → DTE**	
Call Request Call Accepted	Incoming call Call confirmation	Zestawienie połączenia
Clear Request DTE clear confirmation	Clear confirmation DCE Clear confirmation	Rozłączanie połączenia
DTE data Interrupt request	DCE data Interrupt confirmation	Data transfer
DTE receiver ready DTE receiver not ready DTE reject Reset request DTE Reset confirmation	DCE receiver ready DCE receiver not ready Reset indication DCE reset confirmation	Sterowanie przepływem
Restart request DTE restart confirmation	Restart indication DCE restart confirmation	Synchronizacja procesów
Diagnostic	Diagnostic	Raportowanie błędów sieci

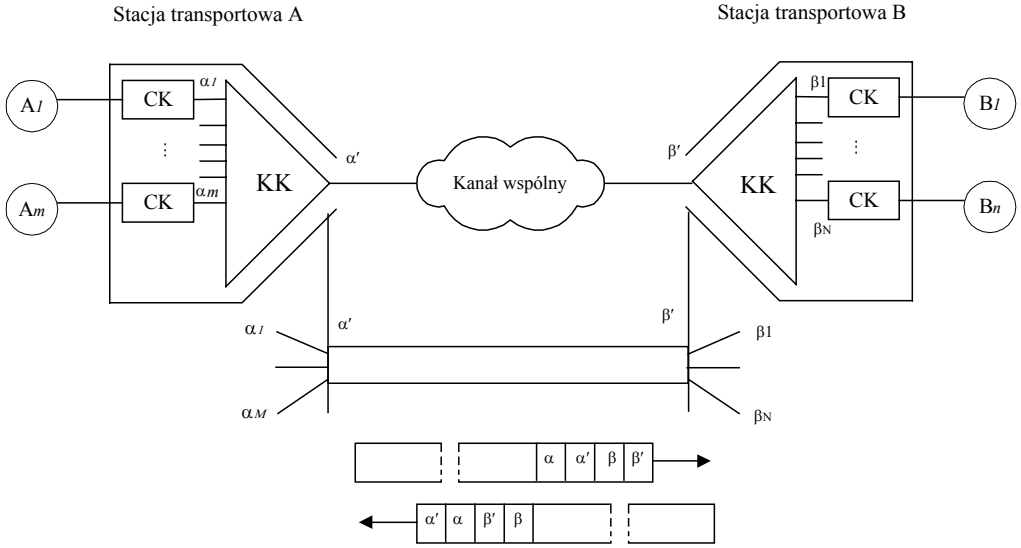
Pole rozszerzenia w pakietach CALL REQUEST i CALL ACCEPTED umożliwia negocjację (pomiędzy stacjami końcowymi) parametrów połączenia, mogą to być: wybór prędkości, wybór sekwencji pakietów, wybór rozmiaru okna i długości pakietu oraz inne. Pakiety diagnostyczne są używane przez węzły sieci do informowania użytkowników DTE o przyczynach wykrytych błędów, np.: błędna sekwencja numeracyjna odbiorcza, nadawcza, błędny typ pakietu, problemy w zestawieniu połączenia i inne.

Połączenie wirtualne

Przed przystąpieniem do omówienia procesów zachodzących w węzłach sieci X.25, celem przybliżenia procesu identyfikacji połączeń występujących pomiędzy dwoma współpracującymi ze sobą abonentami, zostanie omówiony model współpracy dwóch stacji transportowych wykorzystujących wspólny kanał telekomunikacyjny (rysunek 5.4).

Załóżmy, że w ramach stacji transportowych wymieniane są wiadomości w relacjach A_1 z B_1 oraz A_m z B_n. Proces wymiany wiadomości w pierwszej relacji odbywa się z wykorzystaniem CK i identyfikatora relacji α. Człon komunikacyjny może być identyfikowany z punktem dostępu do usług, którego identyfikatorem w relacji z B_1 jest $\alpha 1$. Wiadomości pochodzące z A_1 kierowane są przez koncentrator kanałów logicznych do portu wyjściowego, do którego przyłączony jest kanał łączący go z odległym KK. W związku z tym, że informacja musi być jednoznacznie zaadresowana, w wiadomości pierwotnej pojawia się sekwencja opisująca identyfikator procesu współpracującego w stacji transportowej docelowej. W omawianym przypadku jest to identyfikator $\beta\beta'$. Jednocześnie wprowadzana jest także informacje na temat procesu stacji wysyłającej wiadomość tzn. $\alpha\alpha'$. Wiadomości generowane w relacji przeciwnej adresowane są analogicznie określając dokładnie stacje współpracujące ze sobą.

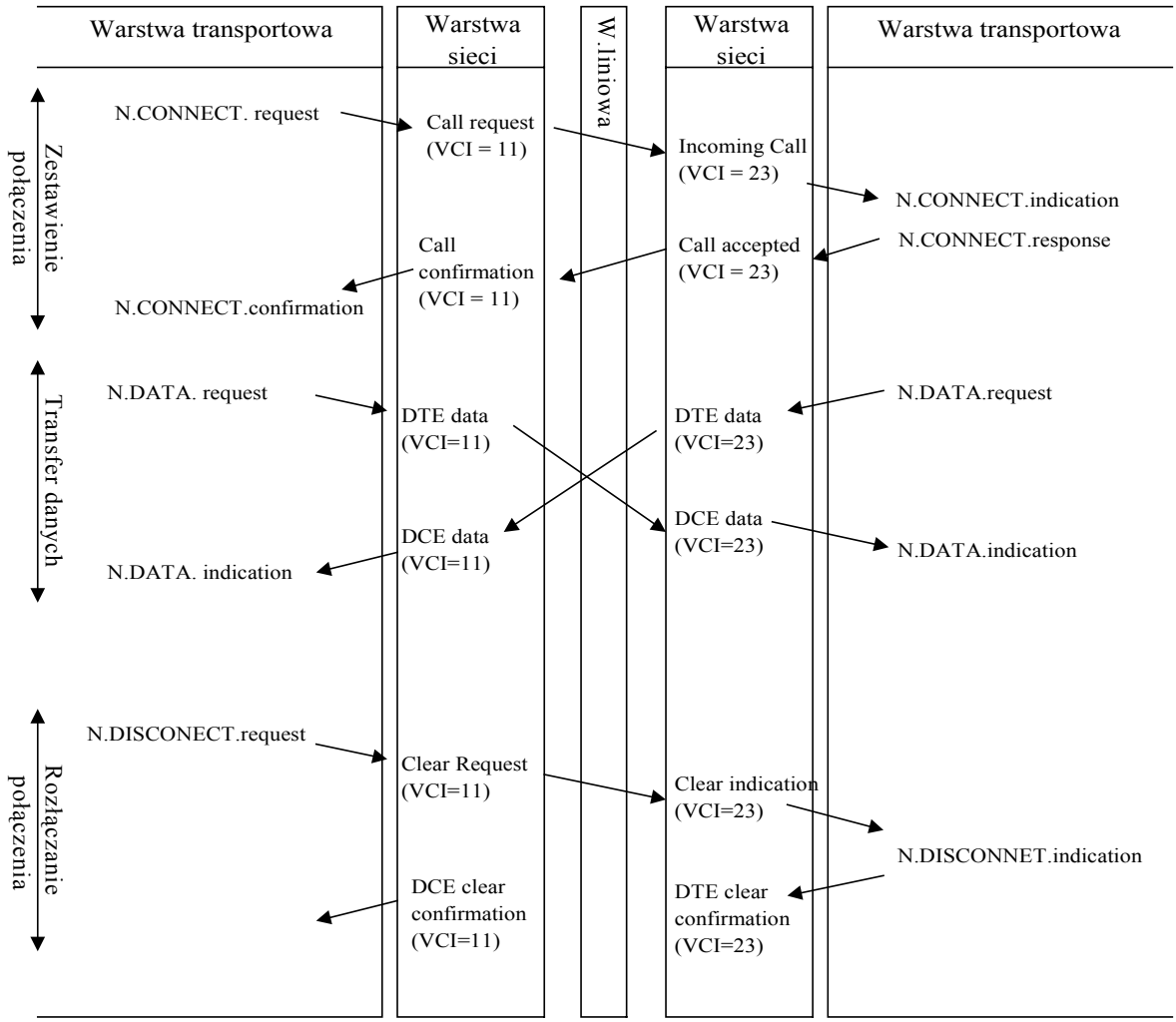
Wiadomości przesyłane są wspólnym kanałem telekomunikacyjnym, w którym równolegle (choć w większości przypadków nie jednocześnie) przesyłane są wiadomości pochodzące z innych relacji współpracujących ze sobą aplikacji. W omawianym przypadku jest to np. relacja A_m z B_n.



Oznaczenia
Koncentrator kanałów logicznych - KK
Człon komunikacyjny - CK
Procesy komunikacyjne - A*m*, B*n*

Rysunek 5.4 Komunikacja procesów aplikacyjnych pomiędzy urządzeniami końcowymi wymieniającymi informację w kilku kanałach wirtualnych zrealizowanych na bazie wspólnego kanału fizycznego

Przystąpmy do omówienia procesów realizowanych w relacji pomiędzy abonentami sieci X.25. Na rysunku 5.5 przedstawiono różne fazy realizacji połączenia.



Rysunek 5.5 Fazy wymiany informacji pakietowej X.25 w kanałach wirtualnych SVC pomiędzy DTE (urządzeniami końcowymi) z uwzględnieniem procesów w warstwie transportowej i sieciowej

W celu zestawienia połączenia jako rezultat generowana jest funkcja elementarna N.CONNECT.request w punkcie dostępu do usług użytkownika. Parametry, które są związane z tą funkcją to adres NSAP wywoływanego DTE i wielkość pola użytkownika. W celu zestawienia połączenia pomiędzy abonentami można wykorzystać dwie procedury. W pierwszej połączenie jest zestawione po wygenerowaniu funkcji elementarnej N.CONNECT.request i wysłaniu odpowiedniego pakietu warstwy sieciowej. Drugą metodą jest alternatywny tryb "fast select", w którym bezpośrednio kierowany jest pakiet call request do stacji docelowej, na który funkcja elementarna N.CONNECT.response generuje pakiet zgody na połączenie.

Chociaż usługi zorientowane połączeniowo odpowiadają aplikacjom, które wymieniają pomiędzy sobą znaczne wielkości danych, wiele spośród programów użytkowych wymaga usług typu szybki wybór – *ang. fast select*. Dla przykładu można posłużyć się przykładem autoryzacji karty kredytowej dokonywanej w czasie transakcji. W przypadku tym nie jest konieczne zestawianie połączenia wirtualnego.

W trybie szybkiego wyboru zarówno pakiety call request i call accepted oraz clear request i clear accepted zawierają pole danych użytkownika o wielkości do 128 bajtów. Po odbiorze danych z funkcji potwierdzenia incoming N.CONNECT.indication, adresat odpowiada funkcją N.DISCONNECT.request z wiadomością odpowiedzi w polu

danych użytkownika. Wiadomość ta transportowana jest do źródła w pakiecie clear request/confirmation, które jednocześnie rozłączają połączenie wirtualne.

Operacja wyboru pierwszego następnego wolnego identyfikatora połączenia wirtualnego VCI (*ang. Virtual Connection Identifier*) i utworzenie pakietu call request zawierającego adres stacji wywoływanej i wywołującej oraz wybranego wcześniej VCI. Pakiet przekazany jest następnie do warstwy łącza danych i stąd poprzez warstwę fizyczną jest on wysyłany do węzła komutacji pakietów wspólnym kanałem. Węzeł po odebraniu pakietu zapamiętuje wykorzystany identyfikator kanału logicznego, sprawdza adres stacji wywoływanej i przesyła pakiet do odpowiedniego portu wyjściowego wg tablicy marszrutyzacji (wybierając wcześniej identyfikator kanału logicznego o najniższym numerze "od góry"). Jednocześnie z powyższymi operacjami pakiet call req zmieniany jest na incoming call. Pakiet przesyłany jest do adresata, do odpowiedniej stacji elementarnej w warstwie sieciowej, gdzie generowana jest funkcja elementarna N.CONNECT.indication, która przesyłana jest do abonenta.

Jeżeli wywołanie jest zaakceptowane przez abonenta, generowana jest funkcję elementarną N.CONNECT.response, która wraca do stacji warstwy sieciowej, która to tworzy pakiet call accepted. Powrotnie wykorzystywany jest, wcześniej zajęty przez pakiet incoming call identyfikator kanału logicznego. Pakiet przekazywany jest do węzła sieci, który zmienia pakiet call accepted w pakiet call connected i przechodzi do fazy transferu danych ustawiając kanały logiczne w stanie transfer danych. Pakiet call connected przesyłany jest do wywołującego DTE. Ostatecznie, po odbiorze pakietu przez DTE źródłowe, stacja elementarna generuje funkcję elementarną N.CONNECT.confirmation do użytkownika (abonenta) i wprowadzana jest faza transferu danych.

Jeżeli abonent docelowy nie zaakceptuje wywołania przychodzącego, wtedy generuje on funkcję elementarną N.DISCONNECT.request. Rezultatem jest wysłanie pakietu clear request do lokalnego węzła komutacji pakietów, który zwalnia identyfikator kanału logicznego do lokalnego DTE, a do odległego DTE wysyła pakiet clear confirmation także zwalniając zarezerwowany wcześniej identyfikator kanału logicznego. Węzeł sieci przekazuje pakiet clear confirmation do stacji inicjującej połączenie. Stacja warstwy sieciowej inicjująca połączenie przesyła do abonenta wywołującego N.DISCONNECT.indication a do węzła sieci pakietowej pakiet clear confirmation po czym zwalniany jest identyfikator kanału logicznego. Podobnie wygląda procedura inicjowania rozłączenia połączenia w fazie transferu danych, czy też w przypadku rozłączenia połączenia przez abonenta wywołującego.

Transfer danych

Po zestawieniu połączenia wirtualnego, każdy z abonentów może zainicjować wymianę danych niezależnie od drugiego, wykorzystując funkcję elementarną N.DATA.request w swoim interfejsie sieciowym. Dane użytkownika są wtedy parametrem funkcji elementarnej. Maksymalny rozmiar pakietu danych jest określony i ograniczony przez sieć komutacji pakietów. Typowa długość pakietu wynosi 128 bajtów. Jeżeli porcja wiadomości zawiera więcej danych, wtedy jest ona wcześniej dzielona na pakiety i każdy z pakietów jest oddzielnie przesyłany w sieci. Przed wysłaniem w każdym z pakietów ustawiany jest bit M-więcej danych (*ang. more data*), jeżeli wymagana jest kompletacja wiadomości przekazywanej do warstwy transportowej u odbiorcy.

Abonenci mogą korzystać bądź z własnego protokołu transferu danych bądź z protokołu oferowanego bezpośrednio przez warstwę pakietową X.25. W pierwszym

przypadku wykorzystywany jest mechanizm bitu Q-kwalifikatora (*ang. qualifier*), który jest ustawiany przez procesy aplikacyjne w urządzeniu abonenckim, w nagłówku pakietu. Po stronie odbiorcy, każdy taki pakiet przekazywany jest bezpośrednio do odpowiedniego procesu.

Zwykle potwierdzanie wymiany danych ma znaczenie lokalne w protokole X.25, ale istnieje także możliwość korzystania z udogodnienia pozwalającego na potwierdzanie danych pomiędzy abonentami końcowymi. Protokół ten jest udostępniany przez procedurę bitu D-potwierdzenia dostarczenia informacji (*ang. delivery confirmation*). Bit D w nagłówku pakietu danych jest ustawiony, gdy wymagane jest potwierdzanie poprawnego przekazania informacji pomiędzy abonentami końcowymi.

Sterowanie przepływem

Wszystkie pakiety warstwy pakietowej są przesyłane pomiędzy DTE a węzłem sieci pakietowej przy wykorzystaniu usług dostarczanych przez warstwę liniową. Wykorzystanie protokołu HDLC powoduje, że dostarczone dane są przesyłane stosunkowo wiernie. W związku z tym w warstwie pakietowej występuje raczej sterowanie przepływem niż kontrola błędów. Algorytm sterowania przepływem bazuje na mechanizmie okna sterowania przepływem. Przepływ pakietów kontrolowany jest oddzielnie dla każdego kanału wirtualnego i dla każdego kierunku wywołania, zarówno w węźle komutacji pakietów jak i w urządzeniu DTE. Wszystkie pakiety danych zawierają numer sekwencji wysłanej P(S) i numer sekwencji odebranej P(R). P(R) zawarty w każdym pakiecie odnosi się do pakietów danych przesyłanych w przeciwnym kierunku. Jeżeli nie ma pakietów danych do nadania, P(R) może być przesłany w specjalnym pakiecie nadzorczym RR. Pierwszy pakiet w każdym kierunku (z DTE do węzła, czy z węzła do DTE) zaopatrzony jest w P(S) równy zero, następny pakiet przesyłany w tym samym kierunku zawiera P(S) zwiększane o jeden. Liczba pakietów związanych z tym samym wywołaniem, które mogą być przesłane w tym samym kierunku w kanale wirtualnym przed pakietem potwierdzenia równa jest rozmiarowi okna K. Jeżeli inicjujący tryb transferu danych osiągnął rozmiar okna, to dopóki nie otrzyma pakietu danych bądź pakietu nadzorczego RR z numerem P(R) wskazującym na odebranie pakietów poprzednich, nie może wysyłać następnych pakietów danych. W celu implementacji mechanizmu okna sterowania przepływem zarówno DTE jak i węzeł sieci posługują się trzema zmiennymi dla każdego kanału logicznego:

- V(S): zmienna sekwencji wysyłania wskazująca numer P(S), który będzie przypisany następnemu pakietowi wysyłanemu w kanale logicznym.
- V(R): zmienna sekwencji odbierania, wskazująca numer P(R) następnego w kolejności pakietu danych, który będzie odebrany w kanale logicznym.
- V(A): zmienna potwierdzenia wykorzystywana do wskazania, kiedy sterowanie przepływem powinno być zakończone.

Wszystkie zmienne są ustawione na 0 zaraz po zestawieniu połączenia, przed przejściem do stanu transferu danych. Zmienne te są zerowane w stanie zerowania (*ang. reset*) kanału logicznego. W czasie przygotowywania pakietu danych do wysłania, przypisywany mu jest numer sekwencyjny P(S), równy aktualnemu numerowi V(S). Jest on później zwiększany modulo-8 albo modulo-128 (jeśli zdefiniowane to jest w polu GFI nagłówka pakietu). Po odbiorze każdego pakietu danych albo pakietu nadzorczego sterowania przepływem RR, numer sekwencji odbiorczej P(R) jest użyty do uaktualnienia V(A). Wysyłający może kontynuować wysyłanie pakietów dopóki nie zostanie osiągnięta górna krawędź okna (zachodzi to wtedy, gdy zwiększana o 1

wartość V(A) osiągnie K) lub też, gdy odebrany pakiet danych albo pakiet RR zawierający P(R) zwiększa aktualną wartość V(A). Tak, więc pakiety danych mogą być przesyłane aż do osiągnięcia nowej wartości granicznej. Typową sekwencję sterowania przepływem przedstawiono na rysunku 5.6. Dla jasności procesu, przedstawiono pojedynczy kanał logiczny z jednokierunkową sekwencją sterowania pakietami.

Wykorzystanie mechanizmu okna do sterowania przepływem podyktowane jest koniecznością zapewnienia odpowiedniej wielkości buforu na przyjęcie pakietów. W praktyce całkowita wielkość buforów przeznaczonych do zabezpieczenia wszystkich wywołań (które są aktualnie aktywne) często jest mniejsza niż wymagane maksimum. Udogodnienie występujące w protokole pozwala DTE lub też węzłowi sieci, tymczasowo zawieszać sterowanie pakietami danych w danym połączeniu logicznym. Jest to realizowane przez wykorzystanie w kanale logicznym pakietu RNR - odbiornik niegotowy (*ang. receiver not ready*). Każdy pakiet RNR zawiera P(R), który określa nową wartość V(A) dla tego kanału. Po odbiorze przez pakietu RNR, wysyłający musi przerwać transmisję dalszych pakietów dopóki ich odbiorca nie będzie gotowy do ich odbioru w tym kanale logicznym. Zazwyczaj przesyłanie jest wznawiane po otrzymaniu przez wysyłającego pakietu RR.

Przedstawiono to w części "b" rysunku. Z rysunku można odczytać, że pakiet RNR nie mógł bezpośrednio wpłynąć na zatrzymanie przepływu pakietów, dopóki pakiet sterowania nie został odebrany. Każdy pakiet odebrany w takim przypadku jest akceptowany, pod warunkiem jednak, że nie nastąpił żaden błąd w warstwie pakietowej. Mechanizmy dotyczą pakietów danych przesyłanych w kanale logicznym, istnieje jednak uprzywilejowana sytuacja, w której DTE może wymienić pojedynczy pakiet danych o wysokim priorytecie do korespondującego DTE niezależnie od procedur sterowania przepływem. Pakiet taki nosi nazwę pakietu przerwania (*ang. interrupt packet*). Dopóki pakiet ten nie oddziałuje na mechanizmy sterowania, może on być odbierany poza sekwencją dla innych pakietów danych w połączeniu. Po odebraniu pakietu przerwania, odbierające DTE (warstwa pakietowa) musi odpowiedzieć pakietem potwierdzenia przerwania (*ang. interrupt confirmation*). Sytuacja wymiany pakietu przerwania może zdarzyć się jedynie raz na jakiś okres czasu danego połączenia wirtualnego.

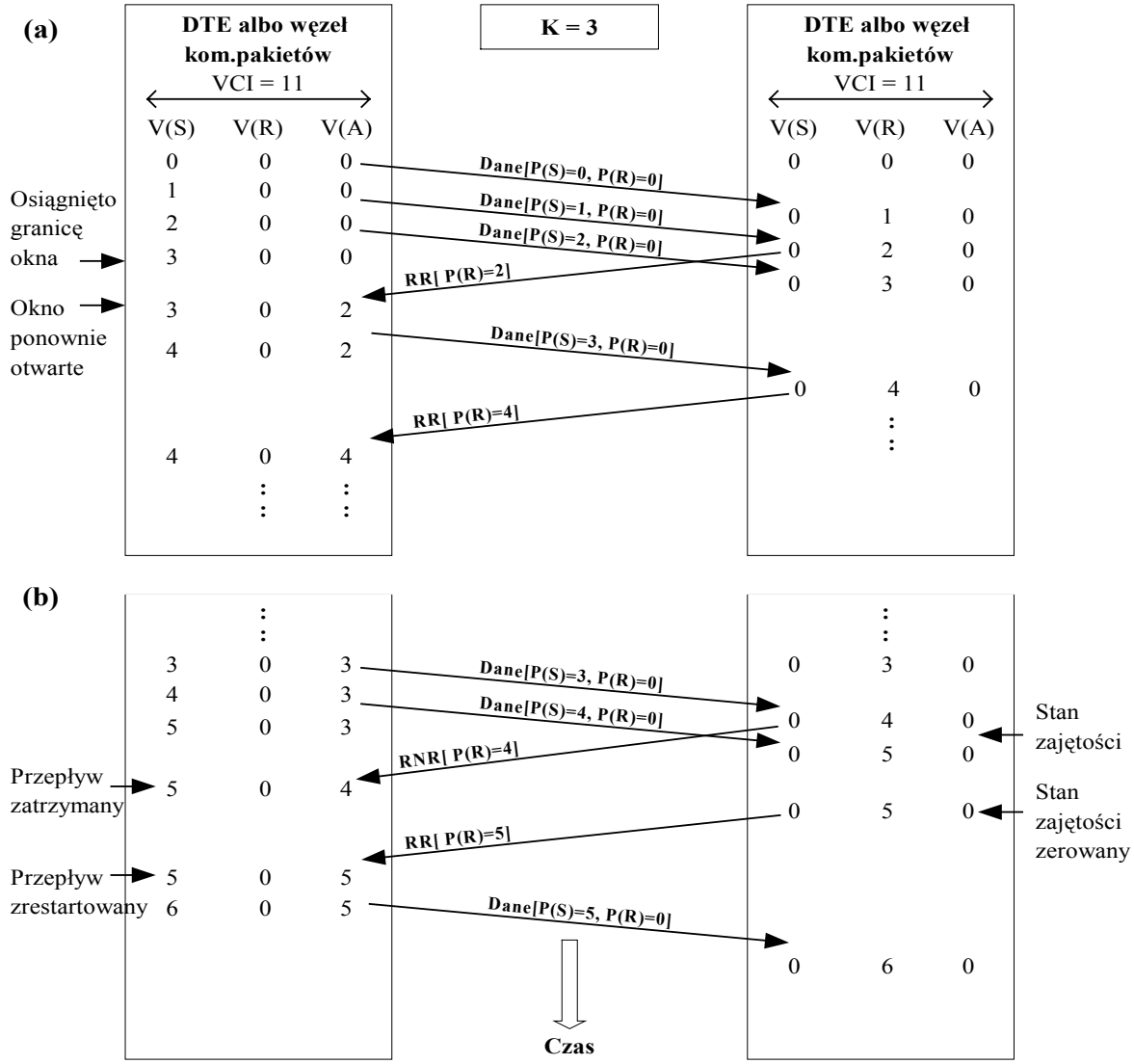
Obsługa błędów

Głównymi mechanizmami związanymi z obsługą błędów warstwy pakietowej są procedury zerowania i ponownego startu (*ang. restart*). Procedura zerowania jest wykorzystywana tylko w fazie transferu danych i tylko w pojedynczym kanale logicznym. Procedura ponownego startu wykorzystywana jest dla wszystkich połączeń wirtualnych danego połączenia fizycznego. Pakiet żądania zerowania połączenia wirtualnego jest wysyłany przez odbierające DTE, w przypadku, gdy odebrany przez nie pakiet jest poza granicami określonymi przez aktualne okno sterowania. Wskazuje to, że obydwa DTE są w stanie rozsynchronizowania a proces sterowania przepływem musi być na nowo uruchomiony.

Wszystkie pakiety przebywające aktualnie w ścieżce połączenia wirtualnego są odrzucone przez warstwę pakietową, użytkownik zaś jest poinformowany o procesie zerowania ("sprzątania") połączenia wirtualnego. Warstwa transportowa zaś odpowiedzialna jest za odzyskanie utraconych danych.

Procedura ponownego startu jest podobna do kasowania wszystkich połączeń wirtualnych będących aktualnie w realizacji. Jest ona wykorzystywana w przypadku utraty synchronizacji w takim stopniu, że dotyczy to wszystkich aktywnych połączeń.

Dla przykładu można podać zdarzenie odebrania przez DTE od węzła sieci pakietu incoming call w kanale wirtualnym, który jest aktualnie w użyciu.



Rysunek 5.6 Przykład sterowanie przepływem (a)operacja okna;(b) operacja RNR

Dostęp do usług sieci X.25

Przedstawione powyżej informacje dotyczą dostępu do usług sieci pakietowej realizowanego z "inteligentnych" DTE, posiadających zaimplementowane procedury warstwy sieciowej a także warstwy transportowej (Rysunek 5.7). Sytuacja taka ma miejsce w przypadku, gdy DTE jest komputerem. Jednak w wielu przypadkach DTE nie może pracować w trybie pakietowym albo nie posiada odpowiednich możliwości do implementacji protokołu takiego jak X.25. By dołączyć takie DTE do sieci wykorzystywane jest dodatkowe urządzenie, które ma zaimplementowane różne warstwy protokołu. Zapewnia ono bardziej prosty styk DTE z siecią. Przykładem takiego DTE jest pracujący w trybie znakowym terminal asynchroniczny np. komputer osobisty czy też prosty terminal ekranowy. Zwykle posiadają one ograniczony poziom inteligencji i prosty interfejs fizyczny np. RS-232C/V.24.

Oczywiście użytkownik zawsze może dokupić odpowiednie urządzenie stykowe, realizujące proces zbierania (asemblacji) znaków z terminala i wysyłające informację w

sieć, a także realizujące proces przeciwny. Jednak nie jest to bezwzględnie niezbędne. Jako rozwiązanie wielu administratorów oferuje protokół dostępu do usług sieci pakietowej zwany X.28. Jest on przeznaczony do obsługi asynchronicznych terminali znakowych. Dodatkowe urządzenie realizujące taki interfejs zwane jest pakietowym asemblerem-dysasemblerem w skrócie PADem (*ang. Packed Assembler - Disassembler*). Gdy PAD zapewniany jest bezpośrednio przez PSPDN to jest on ulokowany w najbliższym węźle komutacji pakietów. Funkcja i lokacja PAD-a zostały przedstawione na rysunku 5.7. Jak można zauważyć, protokół X.3 definiuje operacje i udogodnienia, które są realizowane w PADzie, zalecenie X.29 definiuje zaś interfejs pomiędzy PADem i oddalonym urządzeniem DTE, które pracuje w trybie pakietowym.

Poniżej przedstawiono przykładowe udogodnienia dostępne w sieci X.25.

Korzystanie z numeru skróconego

Abonent sieci X.25 zwykle ma numer 7-mio cyfrowy bez prefiksów. Jednak istnieje możliwość używania numeru 5-cio cyfrowego. Pozwala to na stosowanie dłuższego o dwie cyfry podadresu. Jest to bardzo dobre rozwiązanie dla sieci abonentów podłączonych do POLPAK i pracujących wg protokołu X.25.

Zamknięta grupa użytkowników

Kilku abonentów sieci X.25 może utworzyć grupę. Każdemu członkowi grupy można ustalić określony dostęp w obrębie grupy i poza nią. Szczegółowo można zaprogramować, czy dany abonent może:

- otrzymywać wywołania od abonentów spoza grupy,
- otrzymywać wywołania od abonentów wewnątrz grupy,
- wywoływać abonentów spoza grupy,
- wywoływać abonentów wewnątrz grupy.

Informacje o kosztach połączeń

Po rozłączeniu danego wywołania abonent posiadający to udogodnienie otrzymuje informacje na temat:

- liczby przesłanych segmentów w poszczególnych okresach taryfowych, zgodnie z cennikiem usług sieci X.25.
- czas trwania połączenia.

Na podstawie tej informacji i cennika sieci X.25 abonent może w prosty sposób obliczyć koszt połączenia. Pozwoli to abonentowi na optymalną konfigurację swojego sprzętu, jak również na bieżącą kontrolę miesięcznego budżetu.

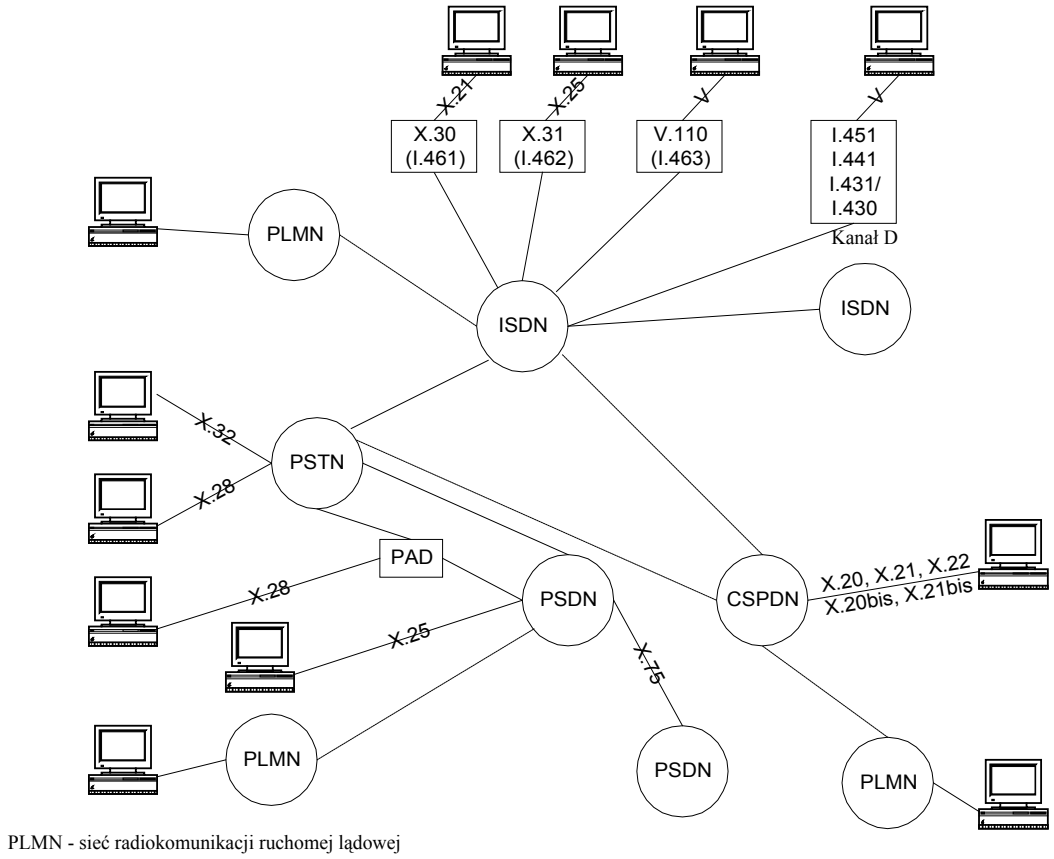
Zakaz realizacji połączeń płatnych

Udogodnienie to pozwala abonentowi na ustawienie w systemie opcji automatycznego zabezpieczenia się przed opłatami za połączenie wychodzące od niego, jak i przychodzące. Wówczas tego typu połączenia odbywają się na koszt odbiorcy lub wywołującego.

Przekierowanie wywołania

Jeśli abonent jest zajęty lub wyłączony, to może sobie zażyczyć, aby wywołania do niego zostały przekierowane do innego, określonego wcześniej abonenta. Abonent korzystający z tego udogodnienia powinien dołączyć do wniosku numer sieciowy

abonenta, do którego nastąpi przekierowanie, oraz informacje na temat warunków powodujących przekierowanie:
- z powodu zajętości abonenta,
- z powodu wyłączenia sprzętu abonenta,
- z powodu zajętości lub wyłączenia.



PLMN - sieć radiokomunikacji ruchomej lądowej

Rysunek 5.7 Organizacja sieci pakietowej

Abonent wielokrotny

Jeśli abonentowi zależy na bardzo wysokiej niezawodności, to może zostać abonentem wielokrotnym. Abonent tego typu posiada urządzenie lub urządzenia końcowe podłączone do co najmniej dwóch węzłów sieci X.25, które są wywoływane jednym numerem. W przypadku awarii jednego węzła lub urządzenia końcowego abonent może nadal odbierać i wysyłać wywołania.

Weryfikacja/identyfikacja użytkownika sieci NUI

NUI jest identyfikatorem użytkownika i umożliwia abonentowi dostęp do sieci X.25. NUI może być również używane przez abonentów w celu zmiany parametrów pracy lub też w celu zapewnienia większego bezpieczeństwa.

Identyfikator abonenta

Indywidualne hasło umożliwiające abonentowi dostęp do sieci X.25. W odróżnieniu od NUI, po podaniu hasła można realizować wiele połączeń w sieci POLPAK podczas jednej sesji telefonicznej. Z hasłem jest związany normalny numer sieciowy sieci X.25 - adres użytkownika sieci. Abonent synchroniczny może być wywoływany za pomocą tego numeru.

Wirtualne sieci prywatne

Udogodnienie sieciowe umożliwiające wydzielonemu użytkownikowi zarządzanie podzbiorem zasobów sieciowych (portów sieciowych) w taki sposób, jak gdyby te zasoby należały do jego osobnej sieci prywatnej.

Automatyczne przełączanie łączy wirtualnych

Ta funkcja podnosi jakość usług świadczonych abonentom. W przypadku awarii węzła tranzytowego lub łącza międzywęzłowego następuje automatyczne przełączanie łączy wirtualnych obsługujących sesje połączeniowe. Mechanizm przełączania jest na tyle szybki, że abonent obserwuje go jako chwilowe zmniejszenie prędkości przepustowości. Z chwilą znalezienia i zestawienia przez sieć nowej drogi obejściowej, praca abonenta odbywa się tak jak przed wystąpieniem przełączenia.

5.2 Frame Relay

Charakterystyka Frame Relay

Frame Relay jest stosunkowo nową, mającą swe źródła w protokole X.25 techniką sieciową pracującą na zasadzie komutacji pakietów. Protokół Frame Relay określony jest zaleceniem CCITT I.122 oraz Q.922, jest to więc sieć ściśle powiązana z koncepcją sieci z integracją usług ISDN (*ang. Integrated Services Digital Network*). W porównaniu do X.25 Frame Relay charakteryzuje się znacznie większymi szybkościami transmisji, mniejszym opóźnieniem wnoszonym przez sieć oraz brakiem algorytmów korygujących błędy transmisji na poziomie warstwy 3 modelu odniesienia OSI/ISO (tabela 5.3).

Tabela 5.3 Porównanie protokołów transmisyjnych X.25, Frame Relay, ATM

	Sieć komutacji pakietów X.25	Frame Relay	Komutacja komórek (cells switching) ATM
Retransmisja pakietów	X	-	-
Znacznik końca ramki	X	X	-
Korygowanie błędów w warstwie 3 OSI/ISO	X	-	-
Wykrywanie błędów w warstwie 2 OSI/ISO	X	X	-

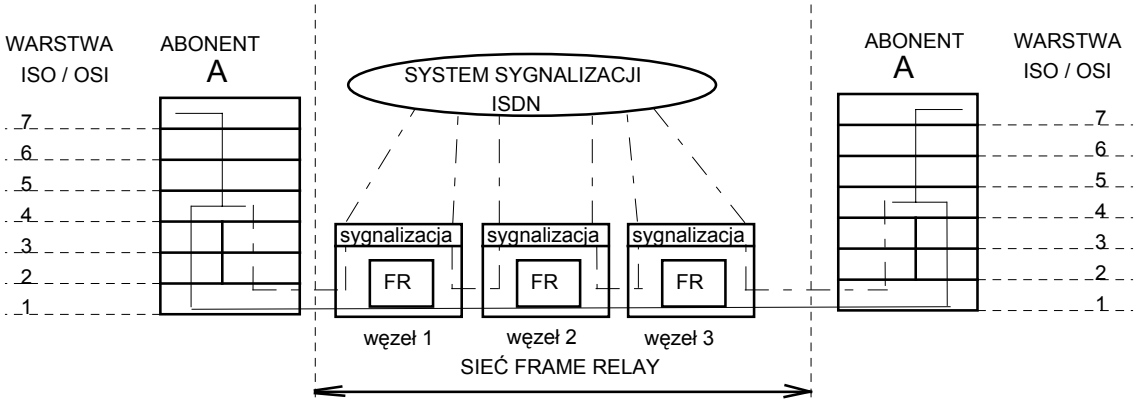
CCITT zrezygnowało z funkcji korekcji błędów w sieci Frame Relay (na rzecz automatycznej retransmisji zniekształconych albo zagubionych pakietów przez protokół abonentów końcowych) mając na względzie znaczny postęp w jakości i niezawodności systemów transmisyjnych. Funkcjonalne charakterystyki Frame Relay oraz jej parametry pozwalają zaliczyć sieci na niej oparte do sieci rozległych WAN. Przewiduje się, że Frame Relay zdominuje rozległe sieci transmisji danych aż do końca bieżącego stulecia, kiedy to prawdopodobnie zostanie ona wyparta przez sieć szerokopasmową z integracją usług opartą na technice ATM (*ang. Asynchronous Transfer Mode*).

Sieć oparta na Frame Relay zbudowana jest z szeregu węzłów - multiplekserów połączonych między sobą liniami transmisji cyfrowej o pojemności do 2.048 Mb/s (trakt E1). Istnieją jednak plany nad zwiększeniem międzywęzłowych szybkości transmisji do 34 Mb/s i wykorzystanie traktów cyfrowych E3.

Topologia połączeń pomiędzy węzłami jest dowolna i powinna zostać zaprojektowana z uwzględnieniem rozbieżności między minimalizacją kosztów a wymaganym stopniem niezawodności.

Frame Relay oferuje usługi typu połączeniowego. Wymiana danych pomiędzy użytkownikami musi zostać poprzedzona procesem nawiązywania połączenia. Połączenie to może mieć charakter połączenia stałego PVC (*ang. Permament Virtual Circuit*) albo czasowego SVC (*ang. Switched Virtual Circuit*) podobnie jak to miało miejsce w sieci X.25.

Pierwsze z nich ustawiane jest jeden jedyny raz podczas dołączania użytkownika do sieci, drugie zaś zestawiane jest każdorazowo na żądanie abonenta. Połączenie pomiędzy parą abonentów sieci Frame Relay (w trybie SVC) rozpoczynane jest procesem sygnalizacji pomiędzy użytkownikiem a siecią poprzez kanał sygnalizacyjny typu D. Proces opisany jest w zaleceniu CCITT Q.931. Sygnalizacja pomiędzy węzłami sieciowymi jest w pełni zgodna z sygnalizacją w sieci ISDN. Po ustanowieniu połączenia użytkownicy rozpoczynają transmisję danych w przydzielonym, różnym od kanału sygnalizacyjnego kanale logicznym. Na rysunku 5.8 przedstawiono tryb transmisji danych w sieci Frame Relay.



Rysunek 5.8 Transmisja danych w sieci Frame Relay

Po zestawieniu ścieżki logicznej pomiędzy abonentami wszystkie ramki danego połączenia przesyłane są tą samą drogą identyfikowaną przez pole DLCI (*ang. Data Link Connection Identifier*) nagłówka. Zawartość DLCI jest zmieniana w każdym węźle tranzytowym sieci na podstawie ustalonych w fazie nawiązania połączenia tablic translacji DLCI in-DLCI out. Dobór trasy pakietów na podstawie takiego algorytmu określany jest terminem node by node. Algorytm ma swe źródło w protokole X.25, gdzie opis połączenia logicznego był określony podczas transmisji pakietu Call Request. Numery kanałów logicznych wybierane są z tablic kanałów logicznych i identyfikują one jedynie połączenie między węzłami sąsiednimi (kanał logiczny wyjściowy węzła k wcześniejszego jest identyczny z kanałem logicznym k+1 następnego).

Ponieważ część kanałów logicznych w węźle k+1 do węzła k+2 jest już wykorzystana, węzeł k+1 przydziela pierwszy wolny kanał logiczny między parą węzłów k+1⇔k+2. Proces taki ma miejsce między wszystkimi węzłami od węzła do węzła (node by node) biorącymi udział w łączeniu abonentów. Po zestawieniu połączenia między abonentami końcowymi, pakiety komutowane są między kanałami logicznymi sąsiednich węzłów. Podobnie proces przebiega w protokole Frame Relay,

gdzie pakiety komutowane są zgodnie z identyfikatorami DLCI zawartymi w tablicach marszrutyzacji, są one przydzielane do momentu rozłączenia połączenia.

Abonent nie posługujący się bezpośrednio urządzeniami pracującymi w standardzie ISDN korzysta ze specjalnych adapterów sieciowych.

Niezawodność i bezpieczeństwo danych we Frame Relay

Węzły Frame Relay realizują proces statystycznej multipleksacji. Konieczne jest z tego względu wyposażenie w odpowiedniej wielkości bufory mogące składować nadchodzące ramki do chwili zwolnienia odpowiednich linii wyjściowych. Wielkość buforów w oczywisty sposób wpływa na prawdopodobieństwo zgubienia ramki. Jeśli poziom wypełnienia buforów danego węzła osiąga pewien zdefiniowany próg, sieć informuje wszystkich abonentów korzystających z usług zagrożonego przeciążeniem węzła o konieczności zredukowania wynegocjowanej w procesie nawiązania połączenia szybkości transmisji. Wiadomość taka rozsyłana jest przy wykorzystaniu dwóch bitów nagłówka ramki: bitu CF (*ang. Congestion Forward Notification*) i BF (*ang. Congestion Backward Notification*). Jeśli pomimo podjętych działań obciążenie węzła wciąż wzrasta, węzeł zaczyna porzucać ramki, których nie jest w stanie obsłużyć, poczynając od ramek oznaczonych bitem DE (*ang. Discard Eligibility*) - ramek użytkowników, którzy przekroczyli określoną podczas nawiązania połączenia szybkość transmisji. Wszelkie niedogodności utraty ramki spadają na urządzenia abonenta, sieć nie jest zdolna do przeprowadzenia retransmisji. Ramki porzucane są również w wypadku wykrycia błędu kodu CRC (*ang. Cyclic Redundancy Check*) czyli w wypadku wykrycia przekłamania bitu lub ciągu bitów zawartych w ramce. Ze względu na fakt, że ramki są nienumerowane, utrata jednej z ramek prawdopodobnie wymagać będzie powtórzenia większej części sesji prowadzonej przez abonentów, za co odpowiada warstwa transportowa użytkowników. Bardzo ważnym wymaganiem dla sieci Frame Relay jest wysoka jakość traktów transmisyjnych.

Dzięki ograniczeniu funkcji korekcji błędów w sieci Frame Relay osiągnięto znaczący wzrost współczynnika wykorzystania zasobów sieciowych. Efektywna prędkość wymiany danych między abonentami jest około pięciokrotnie wyższa od prędkości w sieci X.25 wykorzystującej te same zasoby sieciowe.

Bezpieczeństwo danych przesyłanych siecią Frame Relay jest stosunkowo wysokie. Głównie jest to spowodowane tym, że abonenci identyfikowani są przez połączenie end to end (koniec z końcem) w związku, z czym nie jest możliwy przypadek skierowania pakietu do innego abonenta sieci bez świadomego nawiązania z nim połączenia.

Niezależnie od powyższych możliwości Frame Relay ma zdolność do tworzenia i zabezpieczenia wirtualnych sieci prywatnych, tworzenia zamkniętych grup użytkowników (*ang. Closed User Group*), których przynależność do CUG nie jest ograniczona położeniem w sieci.

Usługi Frame Relay

Frame Relay jest siecią o charakterze połączeniowym, na tej bazie możliwe jest utworzenie sieci z integracją usług. Należy jednak pamiętać, że ze względu na stosunkowo małą prędkość transmisji Frame Relay nie jest w stanie zapewnić możliwości organizowania dużych telekonferencji lub transmisji sygnału wizji wysokiej jakości. Znaczące zmiany w możliwościach tej sieci mogą nastąpić po wprowadzeniu na rynek zapowiadanych multiplekserów Frame Relay pracujących z traktami E3 (34M/s).

Frame Relay często bywa wykorzystywana do łączenia sieci lokalnych i miejskich oraz jako sieć transmisji danych o charakterze sieci rozległej. Sieć ma dużą szansę zdobycia znaczącej pozycji na rynku dzięki cechom umożliwiającym jej ewolucję w kierunku szerokopasmowych sieci z integracją usług B - ISDN. Wydaje się, że obecnie Frame Relay wypiera z rynku europejskiego rozwiązania oparte na zaleceniach X.25 i stanowi pomost dla wprowadzenia sieci ATM.

5.3 ATM

Organizacje standaryzacyjne, w tym CCITT zaproponowały technikę komutacji i transmisji zwaną ATM asynchroniczny tryb transferu (*ang. Asynchronous Transfer Mode*). Osiągnięto już zgodę, co do tego, że przyszła sieć zintegrowana B-ISDN opierać się będzie na tej technice transferu. W środowisku technicznym przyjęły się terminy N-ISDN (*ang. Narrowband ISDN*) i B-ISDN (*ang. Broadband ISDN*) w celu wyodrębnienia tej części ISDN, która związana jest z techniką ATM. W CCITT używa się wspólnego pojęcia ISDN, jedynie z rozróżnieniem dostępu wąskopasmowego i szerokopasmowego.

Transfer asynchroniczny

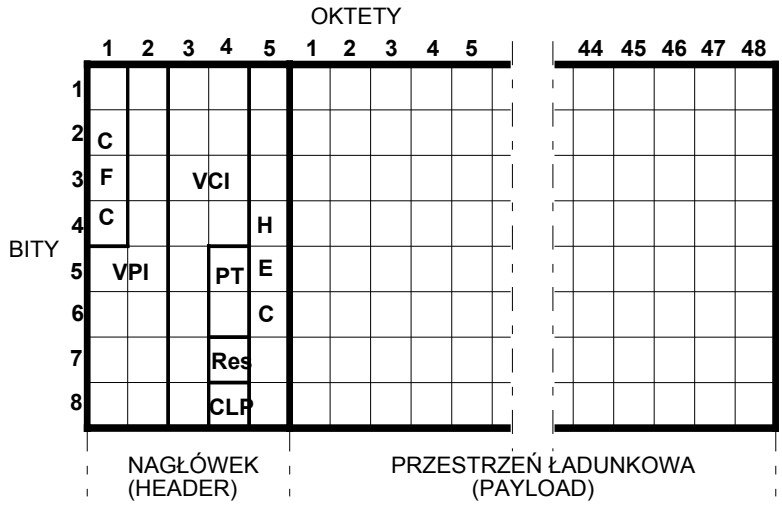
Transfer asynchroniczny jest metodą przekazywania informacji cyfrowej poprzez umieszczanie jej w krótkich pakietach o ustalonej długości, zwanych komórkami (*ang. cells*), lub pakietami ATM. Określenie "transfer" obejmuje zarówno transmisję (a zwłaszcza zwielokrotnienie) jak i komutację informacji, mające na celu przetransportowanie informacji przez sieć telekomunikacyjną, od źródła (nadawcy) do wskazanego ujścia (odbiorcy, ew. odbiorców).

Informacja jest przekazywana w trybie połączeniowym - poprzez połączenia wirtualne zestawiane i rozłączana na żądanie użytkowników. Wywołanie wiąże się z wymianą informacji sygnalizacyjnych pomiędzy abonentem i siecią, umożliwiających uzgodnienie parametrów połączenia wirtualnego. Transfer komórek niosących informację użytkową (a nie sygnalizacyjną) odbywa się po tak utworzonej drodze i nie obciąża sterowania węzłów komutacyjnych. Transfer ma charakter asynchroniczny w tym sensie, że do celów identyfikacji komórki nie jest istotne jej położenie w czasie, lecz informacja zawarta w jej nagłówku. Natomiast transmisja na poziomie komórek (a także na poziomie bitów) odbywa się synchronicznie, jako że komórki mają stałą długość i przylegając do siebie wypełniają kolejne szczeliny czasowe. Na rysunku 5.9 przedstawiono strukturę komórki ATM.

Każda komórka ATM składa się z 5-oktetowego nagłówka i 48 oktetowego pola informacji użytkowej (*ang. payload*). W ramach 40 bitów nagłówka możemy wyróżnić:

- Czterobitowe pole kontroli dostępu GFC (*ang. Generic Flow Control*). Służy ono użytkownikowi do poinformowania sieci o jakości obsługi wymaganej dla danego typu usługi. Pole to występuje tylko na styku użytkownika z siecią UNI (*ang. User Network Interface*) a nie występuje na styku pomiędzy węzłami sieci NNI (*ang. Network Node Interface*);
- Pole numeru ścieżki logicznej VPI (*ang. Virtual Path Identifier*). Komórki należące do tej samej grupy niosą ten sam numer ścieżki logicznej;
- Pole numeru kanału logicznego VCI (*ang. Virtual Circuit Identifier*). Komórki generowane przez tego samego użytkownika oznaczane są tym samym numerem tzw. kanału logicznego.

- Oba pola łącznie pozwalają rozróżniać na styku użytkownika z siecią UNI 2^{24} adresów transakcji; na styku NNI pole VPI jest o cztery bity dłuższe (nie ma pola GFC);
- Dwubitowe pole typu komórki PT (*ang. Payload Type*) pozwala odróżnić komórkę niosącą dane użytkownika (00) od komórki zawierającej informację sygnalizacyjną;
- Jeden bit rezerwy dla przyszłych zastosowań;
- Bit priorytetu CLP (*ang. Cell Lost Priority*). Jeżeli bit ten jest ustawiony na 1 to komórka może być odrzucona w okresie przeciążenia;
- Ośmiobitowe pole kontroli poprawności nagłówka HCS (*ang. Header Check Sequence*).



Rysunek 5.9 Struktura komórki ATM

W ATM stosowane jest zabezpieczenie kodowe nagłówka pomimo spodziewanej wysokiej jakości transmisji. Jest ono konieczne, gdyż pola VCI/VPI stanowią jedyną wskazówkę dotyczącą przeznaczenia komórki, toteż w razie przekłamania komórka trafi do niewłaściwego użytkownika (następuje nie tylko strata informacji, ale i naruszenie prywatności). Zabezpieczenie kodowe nie obejmuje natomiast pola informacyjnego. Nie jest stosowana numeracja komórek ani żadna forma sterowania przepływem; funkcje te, jeśli są konieczne ze względu na charakterystykę usługi, muszą być realizowane przez interakcję źródła i ujścia, bez współdziałania sieci (tj. w trybie end-to-end). Zachowanie kolejności przepływu komórek wynika z natury połączeń wirtualnych.

Transmisja i multipleksacja

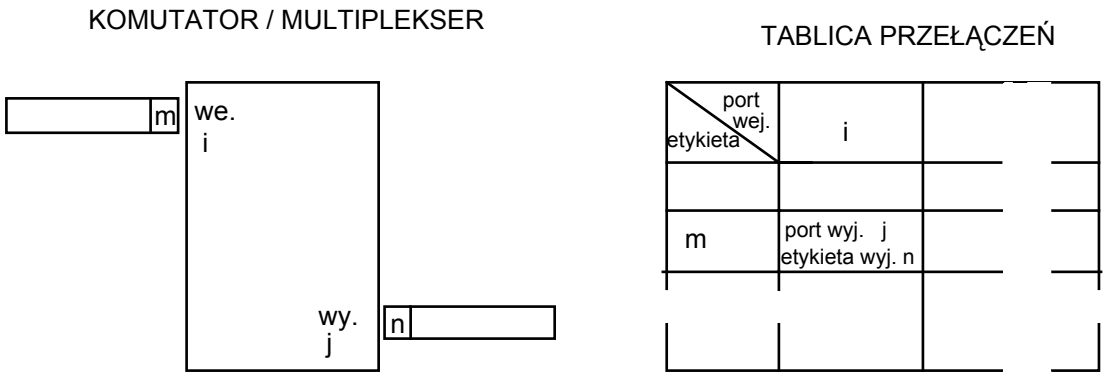
W łączach ATM transmitowany jest ciągły strumień komórek; w razie braku informacji użytkowej wysyłana jest komórka pusta. Nie należy tu mylić szybkości przekazywania danych i szybkości fizycznej transmisji; na znormalizowanym styku abonenta z siecią szybkość transmisji wynosi obecnie 150 Mbit/s, tak więc np. rozmowa telefoniczna wykorzystuje co najwyżej jedną na parę tysięcy komórek nadawanych przez terminal B-ISDN.

Multipleksacja w ATM polega, więc na tym, że do strumienia zbiorczego wprowadzane są tylko komórki "pełne" ze strumieni składowych (w miarę potrzeby uzupełniane komórkami pustymi). Źródła generują komórki w momentach losowych (z punktu widzenia sieci). Ponadto większość usług charakteryzuje się silnie

nierównomiernym napływem komórek tworzących tzw. paczki (*ang. bursts*). Konieczne jest więc kolejkowanie komórek w komutatorze/multiplekserze w celu wyrównania fluktuacji sumarycznej szybkości ich napływu. Jest to źródłem opóźnień szybkości przepływu komórek przez sieć, zaś przepełnienie kolejki powoduje powstawanie strat w strumieniach składowych. Oba te czynniki mają wpływ na jakość transferu. Widoczna jest tutaj wyraźnie fundamentalna różnica pomiędzy ATM a transferem synchronicznym. W ATM zestawienie połączenia (wirtualnego) nie jest równoznaczne z przydzieleniem zasobów sieci w ilości gwarantującej dostarczenie do ujścia całej przekazanej przez źródło informacji.

Komutacja

Informacja zawarta w polu nagłówka nie jest szczegółowym adresem pakietu, lecz tylko etykietą. Operowanie szczegółowym adresem nie jest możliwe z powodu użycia krótkich pakietów. Proces komutacji realizuje się w następujący sposób (rysunek 5.10).



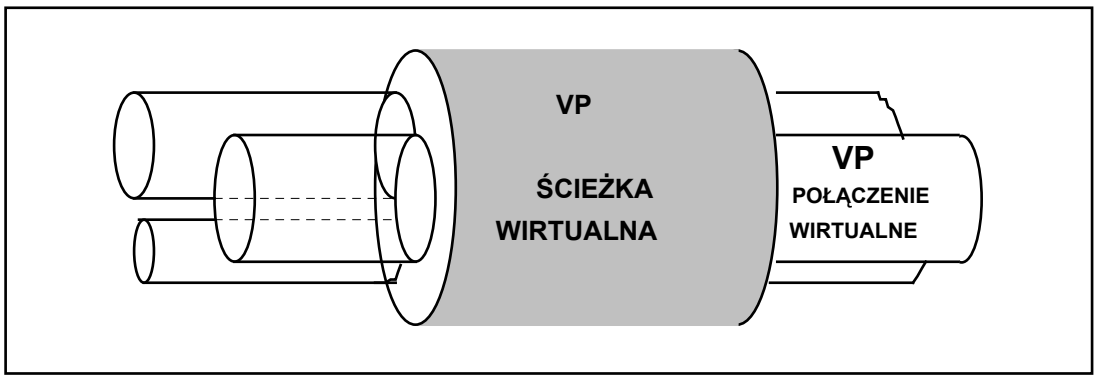
Rysunek 5.10 Zasada działania komutatora/multipleksera ATM

Punkt komutacyjny (komutator/multiplekser) czyta zawartość etykiety komórki m z portu wejściowego, po czym porównuje ją z tablicą przełączeń dla określenia portu wyjściowego.

Komórka jest przepisywana na port wyjściowy j po zastąpieniu etykiety m przez etykietę n. Tablice przełączeń muszą być ustalone przed przyjściem komórki. Mogą one być zmieniane w czasie trwania połączenia. Przesłanie pakietu w technice ATM musi być zatem poprzedzone fazą zestawiania połączenia z uwagi na konieczność uaktualniania tablic w punktach komutacyjnych. Na wejściu komutatora nagłówek ATM może być uzupełniany lub zastępowany przez nagłówek komutacyjny, który określa fizyczną drogę połączenia. Wskazywanie fizycznego adresu portu, statusu i priorytetu obsługi może być zawarte w nagłówku komutacyjnym w powiązaniu z innymi stosownymi informacjami. Struktura i rozmiar tego nagłówka są właściwe dla danego komutatora i jako takie nie mogą być tematem standaryzacji.

Istnieją dwa poziomy połączenia zdefiniowane przez CCITT (rysunek 5.11):

- połączenie typu kanału wirtualnego VCC (*ang. Virtual Channel Connection*);
- połączenie typu ścieżki wirtualnej VPC (*ang. Virtual Path Connection*).



Rysunek 5.11 Rodzaje połączeń ATM

Połączenia typu kanału wirtualnego stanowią podstawowy typ połączenia. Łącze kanału wirtualnego istnieje pomiędzy dwoma punktami komutacyjnymi i jest zdefiniowane poprzez informację zawartą w nagłówku zarówno w polu VCI jak i VPI. Połączenie takie jest ciągiem łączy kanałów wirtualnych istniejących pomiędzy punktami komutacyjnymi. Jest to połączenie typu end-to-end. Niedogodnością związaną z takimi połączeniami jest konieczność przetwarzania dużych ilości informacji w komutatorach z powodu wykorzystywania pól VCI i VPI. Z tego samego powodu wymagane jest użycie dużych tablic przełączeń. Jest to szczególnie ważne w przypadku, gdy węzeł przenosi dużą liczbę połączeń o małej szybkości, jak np. połączenia telefoniczne.

Połączenie typu ścieżka wirtualna utworzone jest z szeregu połączeń typu kanał wirtualny komutowanych jako jedno połączenie. W tym przypadku w procesie komutacji wykorzystywana jest jedynie informacja zawarta w polu VPI nagłówka komórki. W komutatorze VP wszystkie połączenia kanałów wirtualnych z tym samym VPI są komutowane razem.

Można zatem stwierdzić, że rozróżnia się dwa poziomy połączeń ATM: poziom połączenia wirtualnego (poziom wyższy) i zawarty w nim poziom ścieżki wirtualnej (poziom niższy). Elementy komutacyjne poziomu niższego (punkty komutacyjne ścieżek wirtualnych) sprawdzają jedynie część nagłówka zawartą w VPI a elementy komutacyjne poziomu wyższego (punkty komutacyjne połączeń wirtualnych) sprawdzają całe pole przełączeń VPI+VCI. Połączenie typu ścieżki wirtualnej może być użyte jako pewna alternatywa dla łączy dzierżawionych dla połączeń pomiędzy węzłami tworzącymi sieć prywatną. Połączenia ścieżek wirtualnych nie są zdefiniowane jedynie dla styku użytkownik-sieć, ale mogą być także zdefiniowane w styku sieć-sieć. Mogą być one użyte w celu zorganizowania bezpośredniego połączenia przechodzącego przez całą sieć. Mogą być one również użyte do dostarczenia uprzednio zdefiniowanej ścieżki dla funkcji nakładkowych, takich jak usługi bezpołączeniowe.

Sygnalizacja

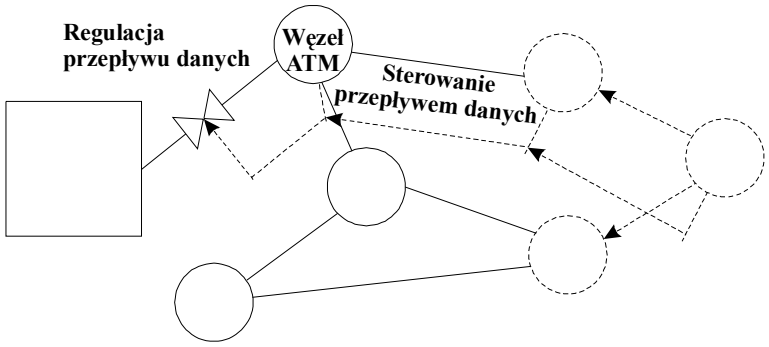
Zestawianie połączeń i ich zwalnianie wykonywane jest przy użyciu specyficznego połączenia ATM, nazywanego Wirtualnym Kanałem Sygnalizacyjnym SSVC (*ang. Signalling Virtual Channel Connection*). Kanał SVCC stanowi połączenie punkt-punkt pomiędzy terminalem i funkcją obsługującą połączenia (umieszczoną na styku użytkownik-sieć lub w głównej centrali). Kanał SVCC jest podobny do kanału D, używanego do N - ISDN, ale z tą różnicą, że każdy terminal ma swój SVCC.

Sterowanie przepływem w zakresie połączenia

Technika ATM jest pewną odmianą techniki pakietowej, gdzie szybkość kanału (na który nałożony jest ATM) jest o wiele większa niż szybkość realizowanych połączeń. Istnieje zatem konieczność sterowania przepływem informacji dla wszystkich połączeń dostępowych. Istniejące sieci pakietowe używają pewnych rodzajów technik sterowania, opartych na sterowaniu szerokością okna, zarówno dla komunikacji międzywęzłowej jak i dla komunikacji użytkownik-węzeł. W przeciwieństwie do powyższego poziom ATM używa sterowania pomiędzy użytkownikiem i siecią (rysunek 5.12).

Wybór mechanizmu sterowania wynika z następujących przesłanek:

- mechanizmy sterowania oparte na ustaleniu szerokości okna nie są odpowiednie dla takich usług, dla których istnieją silne ograniczenia czasu rzeczywistego (mowa, wideo);
- wartość czasu propagacji jest niezależna od szybkości łącza i staje się istotna w przypadku B - ISDN.



Rysunek 5.12 Sterowanie przepływem w ATM

Każde nawiązanie połączenia (VPC czy też VCC) jest poprzedzone nawiązaniem kontraktu pomiędzy użytkownikiem i siecią. Warunki kontraktu mogą być związane z takimi charakterystykami jak wartość średnia i wartość szczytowa oraz czasem, w którym dane będą przesyłane z szybkością szczytową. Sieć monitoruje wszystkie połączenia z punktu widzenia odchyleń od warunków kontraktu. W przypadku wykrycia odchyleń sieć może odrzucać nadmiarowe pakiety lub naznaczać dla przesłania z niższym priorytetem.

Kryteria jakości obsługi

Wspomniane warunki kontraktu związane z połączeniem odnoszą się także do wartości parametrów określających jakość obsługi. Parametry te związane są z pakietowym charakterem techniki ATM. Należy do nich prawdopodobieństwo strat pakietów wynikające z przepełnienia buforów, występowania błędów w nagłówku pakietu lub błędów transmisji.

Nagłówek ATM zabezpieczony jest kodem cyklicznym, 8-bitowym. Pole danych nie jest zabezpieczone z powodu braku uniwersalnej metody nadającej się do zastosowania dla wszystkich rodzajów usług. Dzięki zabezpieczeniu nagłówka zdarzenia polegające na odebraniu pakietu nie związanego z połączeniem jak również duplikacja pakietu są teoretycznie możliwe, ale mogą wystąpić bardzo rzadko. Zalecane prawdopodobieństwo straty pakietu nie jest jeszcze przez CCITT zdefiniowane. Przewiduje się, że będzie ono wynosiło 10^{-8} dla większości przypadków i 10^{-4} dla niskiej jakości połączeń. Następnym parametrem jest opóźnienie przy przesyłaniu pakietu od końca do końca. Jest ono zmienne, co wiąże się z koniecznością

buforowania. Wynikowa zmienność opóźnienia jest jednym z parametrów określających QOS (*ang. Quality Of Service*). Bufory ATM będą prawdopodobnie małe w większości przypadków, co spowoduje, że wynikowe opóźnienie będzie również małe. Rozważany wskaźnik, określający dozwoloną wartość dla opóźnienia jest taki, że z prawdopodobieństwem mniejszym niż 10^{-8} różnica opóźnienia pomiędzy dwoma pakietami, przesyłanymi w ramach jednego połączenia i przechodzącymi przez 30 buforów ATM, powinna być mniejsza od 1s.

Granice dla maksymalnego opóźnienia zależą od typu połączenia. Inne parametry związane są z dopuszczalną końcową stopą błędów dotyczącą przesyłanych przez sieć danych

Dla połączeń, które wykorzystują bit priorytetu (bit CLP) ustalone są różne wartości dla pakietów przesyłanych z wysokim i z niskim priorytetem. Np. 10^{-8} dla priorytetu wysokiego i 10^{-4} dla niskiego (brane są również pod uwagę bardziej rygorystyczne wymagania). Warto w tym miejscu przypomnieć, że połączenia ATM muszą gwarantować zachowanie kolejności przesyłania pakietów.

Nadzór nad połączeniem

Jedną z najczęściej podnoszonych zalet techniki ATM jest jej spodziewana wysoka efektywność, wynikająca z zajmowania przepustowości łącza jedynie na czas transmisji. Jednakże wykorzystanie tej potencjalnie dużej efektywności wymaga wiarygodnych modeli ruchu związanego z różnymi typami usług. Niestety nie udało się jeszcze sformułować zadowalających reguł oceny zasobów, pozwalających zagwarantować spełnienie wymagań dotyczących jakości obsługi. Jeżeli uwzględnić założenie, że ATM ma być metodą transferu dla wszystkich usług (nawet tych jeszcze dzisiaj nie znanych) zagadnienie to coraz bardziej się komplikuje. Zwróćmy uwagę, że jeżeli chwilowa intensywność napływu komórek przekracza przepustowość łącza, to straty komórek dotykają wszystkich jego użytkowników. Zjawisko takie może wystąpić również wtedy, gdy tylko jeden z użytkowników naruszył warunki kontraktu zawartego z siecią w momencie nawiązywania połączenia. Występują więc poważne, dotychczas nie rozwiązane problemy związane zarówno z ustaleniem zasad negocjacji parametrów połączenia jak i kontroli dotrzymywania wynegocjowanych parametrów. Jest tylko jeden sposób nie wprowadzający ryzyka degradacji jakości: posłużenie się maksymalną szybkością transmisji jako podstawą wymiarowania zarówno zasobów łączy jak i komutatorów. Niestety, w takim przypadku ATM stanie się w istocie nieefektywną i kosztowną metodą komutacji łączy.

Warstwa fizyczna

Warstwa fizyczna oferuje warstwie ATM następujące usługi:

- transmisję poprawnych pakietów
- dostarczenie informacji taktującej.

Już od początku prac standaryzacyjnych nad ATM pojawiły się dwie podstawowe koncepcje. Pierwsza z nich oparta jest na pakietach ATM. Ramki, wykorzystywane przez system transmisyjny pasują dokładnie do formatu pakietów ATM. Innymi słowy, system transmisyjny zapewnia strumień bitów, w którym pakiety ATM są bezpośrednio transmitowane. Różne łącza w takim systemie mogą działać w trybie plezjochronicznym. Druga koncepcja zakłada wykorzystanie Synchronicznej Hierarchii Cyfrowej, SDH. Pakiety ATM są wpisywane w strumień bajtowy, zapewniany przez system transmisyjny. Wszystkie funkcje taktujące i synchronizujące są realizowane

przez system SDH. Wadę stanowi tu dodatkowe sterowanie. Zaletą natomiast jest, że istnieją już działające systemy SDH.

Zauważyć jednakże należy, że ATM może być używany jednakowo dobrze (lecz z innymi przepływnościami) z dowolnym systemem transmisyjnym, w szczególności z plezjochroniczną hierarchią cyfrową.

Dotychczas zdefiniowane zostały dla dostępu dwie wartości przepływności binarnych. Stosują się one zarówno do transmisji pakietów ATM jak i SDH. Dostęp przy 155Mb/s. Wartość ta jest równa przepływności dla poziomu STM-1 SDH. W tym przypadku dostęp jest symetryczny (taka sama przepływność w obu kierunkach). Dostęp przy 622,080 Mb/s. Wartość ta jest równa przepływności dla poziomu STM-4 SDH. W tym przypadku dostęp może być symetryczny, lub też może mieć wartość 622,080 Mb/s w jednym kierunku i 155,520 Mb/s w drugą stronę. Niesymetryczny styk byłby użyteczny np. w przypadku, gdy programy telewizyjne byłyby rozdzielane na styku (z większą przepływnością w kierunku użytkownika).

6 Internet

Internet to "sieć sieci", jego protokoły i w konsekwencji usługi są niezależne od fizycznego medium. Obecna struktura fizyczna Internetu przedstawia się następująco. Niewielkie sieci oraz indywidualni użytkownicy są podłączeni do sieci szkieletowej wolnymi łączami telefonicznymi (komutowanymi lub dzierżawionymi), oferującymi przepustowość od 14kb/s do 128kb/s. Bogatsze firmy dysponują szybszymi podłączeniami z siecią np. 2 i 8Mb/s. Sieć szkieletową na poziomie kraju i świata tworzą szybkie dedykowane łącza naziemne oraz satelitarne o przepustowościach od 1,5 Mb/s do 622 Mb/s. Jak wiadomo, Polska jest połączona ze światem kilkoma łączami o przepustowości rzędu 2 Mb/s. Obrazu dopełniają sieci miejskie skonstruowane z wykorzystaniem technologii FDDI lub ATM.

6.1 Model działania i protokoły telekomunikacyjne sieci Internet

Protokoły TCP/IP zostały opracowane na potrzeby sieci Internet. W wyniku intensywnych prac badawczych i normalizacyjnych stały się standardem komunikacyjnym dla komputerów unixowych i wielu innych systemów komputerowych.

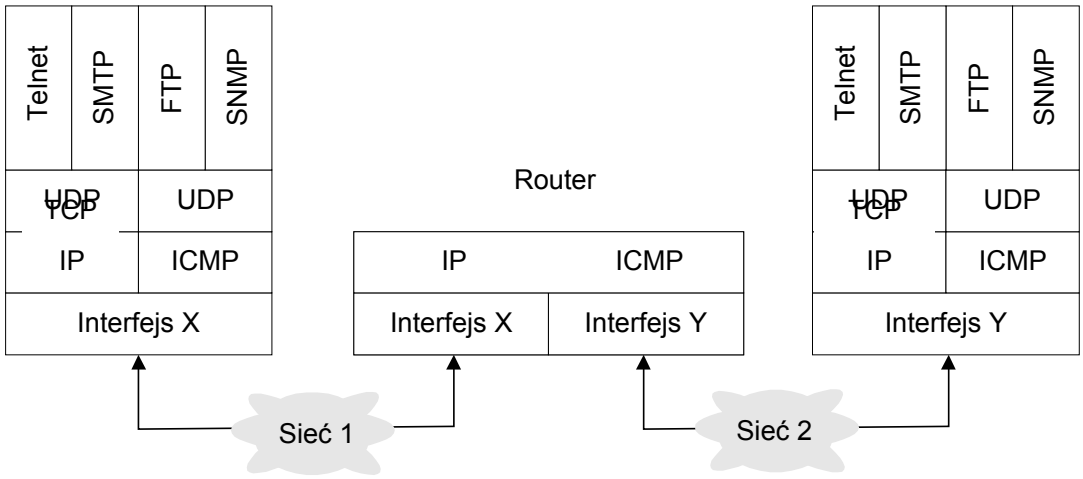
Pod określeniem TCP/IP kryje się jednak więcej niż tylko protokół połączeniowy TCP i protokół bezpołączeniowy IP. Należy raczej mówić o całym zestawie protokołów, przeznaczonych nie tylko do przesyłania danych, ale także do kontroli poprawności połączeń (ICMP), zarządzania siecią (SNMP), usług aplikacyjnych typu FTP (przesyłanie plików) czy zdalnego włączania się do sieci (Telnet). Istnieje wiele różnych protokołów identyfikowanych z zestawem TCP/IP. W krótkim przeglądzie możliwości i właściwości zestawu protokołów TCP/IP ograniczono się do najważniejszych.

W celu pokazania, jak działa sieć wykorzystująca zestaw protokołów TCP/IP przyjmiemy dla uproszczenia, że jako medium komunikacyjne wykorzystywana jest sieć Ethernet. Przyjmijmy także, że korzystamy z możliwości, jakie oferuje program FTP (*ang. File Transfer Protocol*) w celu przesłania pliku w sieci.

Wywołanie usług FTP polega na przesłaniu do zdalnego komputera, na którym uruchamia się serwer FTP odpowiedniego komunikatu zawierającego m.in. adres komputera żądającego przesłania pliku, adres docelowego komputera oraz samo żądanie. Komunikat jest przekazywany do protokołu TCP (działającego w warstwie transportowej modelu sieciowego OSI**),** który dzieli go na segmenty (o długości nie przekraczającej 64 kB), dodaje mu własny nagłówek i przesyła do niższej warstwy sieciowej, to jest protokołu IP.

Protokół IP działa w warstwie sieciowej modelu OSI i stanowi element kluczowy całego zestawu protokołów, gdyż prawie wszystkie komunikaty muszą przez niego przejść. Niezależnie od tego, czy przesyłamy komunikaty lokalnie, czy w sieci rozległej - korzystamy z IP. Protokół IP korzysta z przechowywanej w pamięci tablicy kierowania pakietów określającej, jakiego interfejsu fizycznego powinien użyć do przesłania konkretnego pakietu.

Protokół IP tworzy z segmentów tzw. datagramy tj. dołącza do nich własny nagłówek (zawierający m.in. adres sieciowy IP), niezależny od nagłówka TCP i przekazuje go do niższej warstwy - łącza danych (w naszym przykładzie będzie to zestaw sterowników Ethernetu). Sterowniki Ethernetu przekształcają 32-bitowy adres IP na 48-bitowy adres karty Ethernet (korzystając w tym celu z jednego z protokołów usługowych, a mianowicie ARP *ang. Address Resolution Protocol*) i dodają do komunikatu następny nagłówek (rysunek 6.1) oraz przesyłają pakiet przez fizyczne medium transmisyjne sieci (kabel koncentryczny lub skrętka) do wszystkich komputerów dołączonych do niej. Odbiera go jedynie ten komputer, dla którego komunikat jest przeznaczony pozostałe odrzucają.



Rysunek 6.1 Model warstwowy sieci opartej o protokół TCP/IP

W trakcie przesyłania datagramów przez sieć następuje zwykle ich dalszy podział na fragmenty o długości zależnej od używanej sieci transportującej komunikaty (w przypadku Ethernetu przesyłany pakiet nie może mieć długości większej niż 1536 bajtów).

W komputerze docelowym następuje dokładnie proces odwrotny sterownik Ethernetu usuwa własny nagłówek i przekazuje pakiet do warstwy IP. Warstwa IP usuwa własny nagłówek, składa fragmenty komunikatu w kompletne segmenty i przekazuje je do warstwy TCP, która po usunięciu specyficznego dla niej nagłówka przesyła komunikaty do odpowiedniego programu usługowego (w naszym przykładzie

jest to FTP). Wiele powszechnie znanych programów aplikacyjnych ma przypisany tzw.: numer portu, określający dokładnie ich miejsce i sposób wywołania. Ułatwia to komunikowanie się z nimi. Dla FTP jako numer portu przypisano 20.

Ponieważ w jednej sieci TCP/IP może istnieć wielu użytkowników; którzy próbują komunikować się z jednym programem usługowym, musi on mieć możliwość odróżnienia poszczególnych użytkowników w celu właściwego skierowania odpowiedzi. Zestaw złożony z numeru sieciowego nadawcy, jego numeru portu, adresu sieciowego i numeru portu odbiorcy komunikatu stanowi, tzw. połączenie. W celu obsługi tych wielu połączeń każdy serwer usług tworzy sobie kolejkę komunikatów, które obsługuje w ustalonej kolejności.

Protokół IP

Jest to protokół przesyłający komunikaty w sieci na zasadzie „jeśli się uda, to prześlę". Pakiety danych są wysyłane w sieć bez sprawdzania ich dalszych losów. W efekcie wiadomość może zagubić się w sieci, zostać zniekształcona, przyjść do odbiorcy w kolejności nie mającej związku z kolejnością nadawania, ulec duplikacji, zostać pofragmentowana itp. Jedynie w przypadku pofragmentowania komunikatu zostaje on złożony do początkowej postaci przez IP; pozostałe sytuacje błędnych transmisji muszą być rozstrzygane przez wyższe warstwy protokołu sieciowego lub program aplikacyjny.

Węzeł sieci TCP/IP (stacja robocza, router, serwer) zawiera lokalny bufor danych, w którym zbiera przychodzące komunikaty przed ich przetworzeniem. W razie przepełnienia bufora (większa szybkość przychodzenia komunikatów niż możliwości ich przetworzenia) komunikat jest gubiony bez śladu; w pewnych przypadkach do nadawcy przesyłany jest komunikat ICMP informujący o tym fakcie.

IP nadaje się dobrze do sieci o dobrej niezawodności i dobrej jakości połączeń (zakłada, że wszystkie pakiety przychodzą bez błędów, co najwyżej zostają podzielone na mniejsze na skutek przejścia np. przez sieci lokalne). Wtedy przekazuje komunikaty szybko i z małym narzutem własnym.

Adresowanie IP

Każdy węzeł sieci TCP/IP ma przypisany 4-bajtowy numer identyfikujący zarówno sieć jak i lokalny komputer (host) w sieci. W większości przypadków ten numer jest nadawany węzłom sieci przez administratora, jednakże istnieje możliwość dynamicznego nadawania tego numeru w momencie startu lokalnego węzła sieci (za pośrednictwem protokołu BOOTP) lub dynamicznego "wypożyczania" numeru z puli dostępnych numerów sieciowych (za pośrednictwem protokołu DHCP).

Wyróżnia się cztery klasy adresów w sieci IP dopuszczające różne ilości sieci lokalnych i hostów (rysunek 6.2):

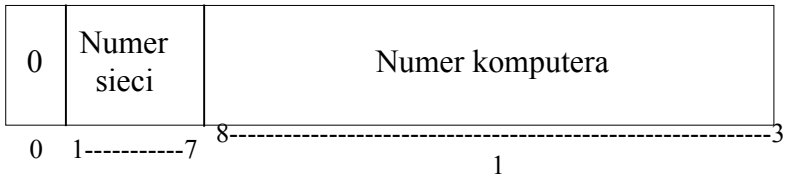
- adres typu A dopuszcza 16 mln hostów ale tylko 127 sieci;
- adres typu B dopuszcza 65 tys. hostów i 16 tys. sieci;
- adres typu C dopuszcza 254 hosty i 2 mln sieci.
- adres typu D (specjalny) służy do rozsyłania komunikatów do wielu węzłów sieci (rozgłaszanie).

Szybki rozwój sieci Internet spowodował, że cztery bajty adresu IP już nie wystarczają i w najbliższym czasie przewiduje się "modernizację" protokołu IP w celu dopuszczenia adresu o większej długości.

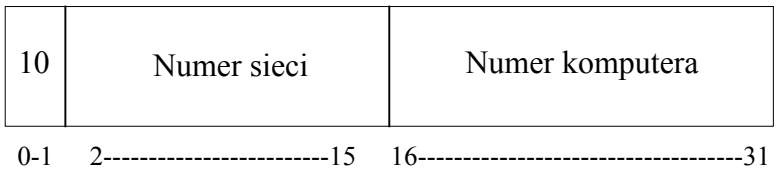
Format datagramu IP

Datagram IP zawiera nagłówek, w który wpisano wszystkie informacje niezbędne do skierowania go od nadawcy do odbiorcy oraz właściwy komunikat. Nagłówek składa się z obowiązkowej części o długości 20 bajtów i części opcjonalnej o długości zmiennej.

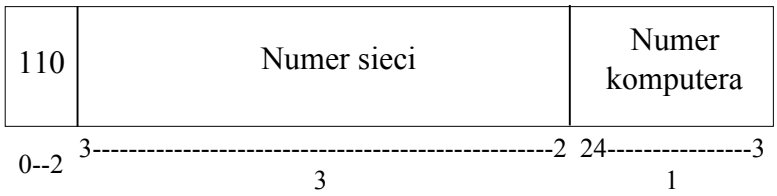
Adres klasy A



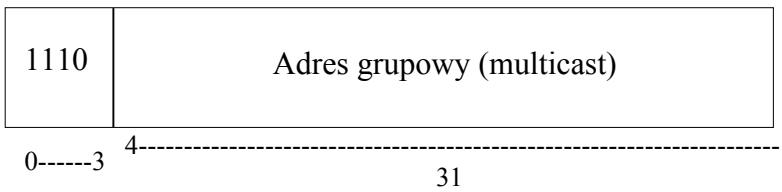
Adres klasy B



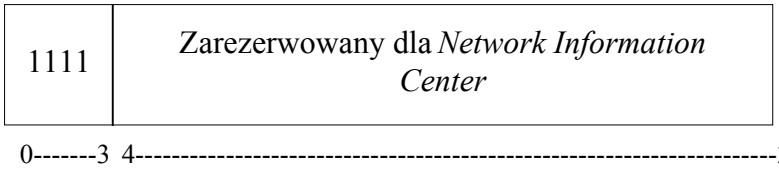
Adres klasy C



Adres klasy D



Adres klasy E



Rysunek 6.2 Klasy adresów w protokole TCP/IP

Część obowiązkowa nagłówka datagramu IP składa się z następujących pól:
- Numer wersji. Umożliwia identyfikację poziomu standardu IP
- Długość nagłówka.
- Typ usług. Pozwala na określenie priorytetu komunikatu.

- Całkowita długość pakietu IP (nie więcej niż 64 kB).
- Pole identyfikacji. Umożliwia poskładanie komunikatów; które w trakcie przesyłania zostały podzielone na mniejsze segmenty.
- Znaczniki. Jeden pokazuje, że pakiet nie powinien być dzielony; drugi wskazuje, że jest to ostatni fragment podzielnego pakietu.
- Offset fragmentu. Pokazuje odległość segmentu danych od początku pakietu; służy do składania pakietów w jeden komunikat.
- Czas życia. Z każdym przejściem pakietu przez węzeł sieci, liczba w tym polu jest zmniejszana o jeden; gdy spadnie do zera - pakiet jest usuwany z sieci. Celem jest uniknięcie krążenia w sieci pakietów, których nikt nie odbiera.
- Protokół. Pole służy do wskazania protokołu, do którego zostanie skierowany pakiet, gdy już zostanie poskładany z fragmentów przez IP Protokół wskazuje się przez nadany mu numer: TCP ma numer 6, UDP - numer 17 a ICMP - numer 1.
- Suma kontrolna nagłówka. Do wykrywania i korekcji jednego błędu nagłówka.
- Adres nadawcy (4 bajty).
- Adres odbiorcy (4 bajty).

Pola opcjonalne w nagłówku pozwalają na wstawienie w nie czasu nadania komunikatu, identyfikację węzłów; przez które pakiet przeszedł i określenie warunków bezpieczeństwa.

Protokół ICMP

Jest ściśle związany z IP i służy do przekazywania komunikatów o nieprawidłowościach w funkcjonowaniu sieci IP. Posługuje się 12 komunikatami, które może wymieniać z węzłami w sieci. W szczególności podaje informacje o przekroczeniu czasu życia pakietu, o powstaniu korka w ruchu pakietów w jakimś węźle, pozwala na wskazanie innej drogi pakietów; na testowanie drożności sieci, na synchronizację zegarów serwerów w sieci i inne.

Protokół TCP

W trakcie przechodzenia pakietów przez sieć mogą one ulec zagubieniu, zostać powielone (dotyczy to zwłaszcza pakietów rozgłoszeniowych - wysyłanych do wszystkich lub dużej liczby węzłów w sieci). Ponieważ przybywają one niezależnie jeden od drugiego - mogą pojawiać się u odbiorcy w przypadkowej kolejności. Protokół TCP uzupełnia możliwości protokołu IP w celu zapewnienia niezawodnej komunikacji od nadawcy do odbiorcy.

TCP ma możliwość otwierania i utrzymywania połączenia (wirtualnego kanału) między nadawcą a odbiorcą oraz przesyłania w nim danych. Realizuje się to za pomocą zbioru prostych operacji, takich jak:

- ustanowienie połączenia,
- akceptacja połączenia,
- wysyłanie danych,
- odbieranie danych,
- zamykanie połączenia,
- awaryjne zamykanie połączenia.

Z tych operacji korzysta się w takich programach jak wspomniany już wcześniej FTP czy Telnet. Protokół IP pozwala na wskazanie połączenia między komputerami w sieci (za pomocą adresu nadawcy i odbiorcy), jednak właściwe połączenie między

programami użytkowymi ustanawia się za pomocą TCP, podając numer portu programu, który wykorzysta przesyłane dane.
Podobnie jak w przypadku datagramu IP komunikat TCP składa się z nagłówka TCP i pozostałych danych.
Nagłówek TCP ma długość co najmniej 20 bajtów i zawiera:

- Numer portu aplikacji u nadawcy i u odbiorcy: Nie jest to jednak adres sieciowy. Dopiero kombinacja numerów portów TCP z adresami sieciowymi IP nadawcy i odbiorcy tworzy tzw. połączenie (zwane inaczej gniazdem - socket).
- Numer sekwencji zawierający informacje umożliwiające zestawienie pakietów we właściwej kolejności i stwierdzenie, czy któregoś brakuje.
- Potwierdzenie pozwalające na przesłanie zwrotne liczby odebranych bajtów i umożliwienie nadawcy powtórnej transmisji zagubionych pakietów.
- Długość nagłówka.
- Kody - służące do wskazania pilnie potrzebnych danych lub podanie, że pakiet kończy dane.
- Okno umożliwiające zwiększenie długości przesyłanego pakietu w celu przyśpieszenia transmisji.
- Suma kontrolna nagłówka do wykrywania i korekcji jednego błędu nagłówka.
- Wskaźnik pilnie potrzebnych danych w przesyłanym pakiecie. Inne pola i nagłówki są opcjonalne i pozwalają m.in. na wskazanie rozmiaru pliku, który będzie przesyłany.

Protokoły połączeniowe i bezpołączeniowe

Protokoły połączeniowe polegają na tym, że sieć przyjmuje odpowiedzialność za dostarczenie komunikatu między nadawcą a odbiorcą. W tym celu urządzenia sieciowe muszą podtrzymywać ciągły dialog, m.in. w celu ustalenia parametrów transmisji, sprawdzania przebiegu pakietów w sieci, sprawdzania ich poprawności, upewniania się, czy przybywają w ustalonej kolejności do odbiorcy itp.

Protokoły bezpołączeniowe polegają na tym, że sieć nie przyjmuje odpowiedzialność za dostarczenie komunikatu między nadawcą a odbiorcą zajmuje się jedynie wysyłaniem pakietów do odbiorcy. Nie sprawdza, czy przybywają do miejsca przeznaczenia, czy są poprawnie przekazane, czy przybywają we właściwej kolejności. Wszystkie te czynności muszą wykonywać odbiorca i nadawca.

Protokoły połączeniowe tworzą między nadawcą a odbiorcą logiczny kanał (zwany czasem kanałem wirtualnym), przez który pakiety mogą przybywać w ustalonej kolejności. Przez ten kanał nadawca i odbiorca utrzymują kontakt w celu wymiany komunikatów o stanie transmisji. Protokoły połączeniowe działają w warstwie transportowej modelu OSI. W celu ustanowienia połączenia aplikacja w komputerze żąda ustanowienia sesji połączeniowej z drugim komputerem za pośrednictwem protokołu TCP. Po ustanowieniu połączenia sieć może przesyłać pakiety z szybkością ograniczoną jedynie przez techniczne właściwości łącza, gdyż w zasadzie nie wymaga kontroli. Po zakończeniu transmisji następuje przerwanie połączenia na żądanie nadawcy lub odbiorcy. W szczególnych przypadkach istnieje możliwość ustanowienia stałego połączenia (odpowiednik linii telefonicznej dzierżawionej).

W protokołach bezpołączeniowych nie ma potrzeby wstępnego negocjowania warunków połączenia. Nadawca rozpoczyna po prostu wysyłanie pakietów danych (zwanych datagramami) w sieć. Odbiorca musi zestawić je we właściwej kolejności (gdyż ze względu na różne drogi w sieci mogą przybywać w dowolnej kolejności),

zażądać retransmisji, jeżeli jakiś pakiet zaginął w drodze. Brak etapu negocjacji wstępnych powoduje, że szybkość przesyłania danych za pomocą protokołów bezpołączeniowych jest większa. Przy dobrym stanie sieci protokoły bezpołączeniowe zapewniają zdecydowanie większą szybkość przesyłania.

Protokół UDP

UDP (*ang. User Datagram Protocol*) został stworzony w celu umożliwienia użytkownikom komputera bezpośredniego korzystania z możliwości bezpołączeniowego przesyłania danych w sieci za pośrednictwem IP. Sprowadza się do nagłówka IP numeru portu programu, z którego komunikat jest wysyłany i numeru portu programu przeznaczenia. Protokół UDP ma takie same właściwości jak IP, chociaż uważa się, że działa na poziomie warstwy transportowej modelu OSI (tej samej co TCP).

Protokoły usługowe

Istnieje wiele protokołów usługowych w zestawie TCP/IP; niektóre z nich są angażowane bezpośrednio w trakcie ustanawiania połączenia przez TCP i przesyłania datagramów przez IP. Inne stanowią dogodne uzupełnienie właściwości funkcjonalnych zestawu w celu ułatwienia przekazywania pakietów przez sieci rozległe zawierające routery: Jeszcze inne służą do zarządzania systemami komputerowymi i sieciami.

Protokół ARP (*ang. Address Resolution Protocol*)

Służy do przekształcenia adresu sieciowego IP (32 bity) na adres fizyczny karty Ethernet, zainstalowanej w komputerze odbiorcy. Istnieją różne metody uzyskania tego adresu. Najszybsza polega na przechowywaniu tabeli odpowiedników często używanych adresów; jednak tabela ma tę wadę, że zajmuje dużo miejsca, jeśli trzeba przechowywać wiele adresów ARP stosuje metodę dynamicznego określania adresu fizycznego. W rym celu rozgłasza w sieci adres sieciowy poszukiwanego komputera i oczekuje na odpowiedź zawierającą jego adres fizyczny.

Protokół RARP (*ang. Reverse Address Resolution Protocol*)

Umożliwia stacji bezdyskowej, włączanej do sieci uzyskanie informacji o jej adresie sieciowym. W tym celu stacja w procesie startu rozgłasza w sieci pakiet Ethernet, zawierający potrzebę uzyskania swego adresu sieciowego. Wyznaczony serwer RARP przesyła do niej jej adres sieciowy.

Protokół BOOTP

Protokół BOOTP został zaprojektowany w 1985 roku (RFC 951) jako usprawnienie protokołu RARP pozwalającego stacji roboczej w sieci TCP/IP uzyskać adres IP BOOTP pozwala także na uzyskanie nazwy i lokalizacji plików na serwerze IP. BOOTP służących do wystartowania bezdyskowych stacji w sieci.

Protokół DHCP (*ang. Dynamic Host Configuration Protocol*)

Rozwinięcie protokołu BOOTP; w zakresie startu stacji w sieci TCP/IP działa tak samo. Umożliwia posługiwanie się ograniczonym zbiorem adresów IP i dynamicznie "wypożycza" je do stacji aktualnie czynnych w sieci, ułatwiając konfigurowanie dużych sieci i przenosząc obciążenie z tym związane z użytkownika na administratora sieci. W celu skonfigurowania serwera DHCP administrator sieci musi mu podać zakres

dopuszczalnych adresów IP zbiór wspólnych dla nich parametrów konfiguracyjnych i czas trwania "wypożyczenia" adresu.

Protokół SNMP (*ang. Simple Network Management Protocol*)

Protokół zarządzania zasobami sieci. Opracowany na potrzeby sieci Internet, chociaż ostatnie wersje działają także dla innych protokołów sieciowych. Jest to popularny protokół do zbierania informacji o węzłach sieci. Informacja jest zbierana przez agentów (programy działające w węzłach sieci) i zapisywana do bazy informacji do zarządzania MIB (*ang. Management Information Base*). Baza MIB ma dobrze zdefiniowany format, może być więc używana przez dowolny system zarządzania zasobami. Wszyscy producenci sieciowych systemów operacyjnych korzystają z SNMP. Większość producentów inteligentnego sprzętu sieciowego (huby, routery, zasilacze UPS) dołącza możliwość uruchamiania agenta SNMP i zarządzania ich produktów przez protokół SNMP. W przypadku urządzeń nie mających agenta SNMP istnieje na ogół możliwość używania tzw. agenta zastępczego (proxy agent) spełniającego te same funkcje.

6.2 Adresacja w sieci TCP/IP

Rozpatrzmy sytuację, w której komputer PC (lub serwer systemu Unix) jest częścią sieci LAN, podłączonej na stałe do Internetu. Każdy z takich komputerów dysponuje, więc kartą sieciową, a administrator sieci w porozumieniu z NIC (*ang. Network Informotion Center*), organizacją przyznającą adresy w sieci Internet przypisuje mu w momencie instalacji oprogramowania sieciowego właściwy adres, a praktycznie trzy adresy. Nie są to jednak trzy odrębne adresy, ale jeden wyrażony na trzy sposoby. Każdy z nich jest wykorzystywany przez inną warstwę modelu OSI do identyfikowania stacji w sieci Internet. Z punktu widzenia użytkownika ważne są tylko dwa adresy używane przez górne warstwy modelu OSI. Trzeci adres, którego format zależy od rodzaju sieci LAN, nie dotyczy użytkownika. Służy on do adresowania stanowisk (kart sieciowych zainstalowanych w komputerach) w konkretnej sieci LAN przez warstwę łącza danych modelu OSI.

Użytkownik posługuje się najczęściej adresem używanym przez aplikacje korzystające z usług sieci Internet. Każdy komputer ma więc przypisaną sobie nazwę składającą się z kilku części oddzielonych znakami kropek. Nazwę komputera i sieci, w której on pracuje, wybiera sobie sam użytkownik przy konfigurowaniu swojej sieci LAN. Nazwa taka może wyglądać następująco *xyz.edu.pl.*

Systemem nazw przypisanych komputerom zarządzają w sieci Internet serwery DNS (*ang. Domain Name System*). Serwery te (których jest bardzo dużo) są zorganizowane w strukturę hierarchiczną, a ich głównym zadaniem jest świadczenie bardzo ważnej usługi: poddawanie konwersji nazwy przypisanej stanowisku na numer protokołu IP. Numer ten jest kolejną (drugą już) formą adresu przypisaną komputerowi. Trzecim rodzajem adresu, przypisanym stanowisku w sieci Internet, jest adres adaptera zainstalowanego w danym komputerze. Adres ten jest stosowany tylko przez warstwę łącza danych modelu OSI i przybiera różne formy, zależne od rodzaju sieci LAN. W sieci Ethernet jest to zawsze 48-bitowa liczba przypisana do konkretnego adaptera sieci. W sieci Token Ring będzie to, oczywiście, adres zupełnie innego formatu.

Jeśli w sieci Internet użytkownik wysyła plik do komputera *abc.edu.pl* (korzystając z protokołu FTP), to kolejne warstwy modelu OSI poddają ten adres konwersji na numer protokołu IP (np. na 12.13.14.15) a w sieci przeznaczenia adres ten jest

zamieniany przez protokół konwersji ARP (*ang. Address Resolution Protocol*) na adres konkretnego adaptera sieci (w sieci Ethernet będzie to 48-bitowa liczba, np. 125739de34d5). Użytkownik może zaadresować stację w sieci Internet wpisując do polecenia jego nazwę lub numer używany przez protokół IP. Ta ostatnia metoda jest dlatego cenna, że można ją użyć w razie braku dostępu do serwera DNS. Każda bowiem nazwa komputera musi zostać przetłumaczona na numer IP przed wysłaniem żądania usługi w sieć. Posługując się bezpośrednio numerami IP, nie korzystamy w ogóle z serwerów systemu DNS.

Adres definiujący sieć (w szczególnych wypadkach podsieć) i komputer w sieci Internet składa się z 32 bitów, które są zapisywane jako cztery liczby dziesiętne oddzielone znakami kropek (np. 12.13.14.15). Każda z tych liczb zwana jest bajtem lub oktetem, ponieważ składa się z jednego bajta, czyli ośmiu bitów. Tak, więc wartość każdej z tych czterech części adresu zawiera się w przedziale liczb 0-255. To, która część adresu, czyli które bajty, określa numer sieci, a która numer komputera, zależy od klasy adresu.

Niezależnie od klasy adresu istnieją pewne stałe reguły kierowania ruchem pakietów, w sieci. Jeśli sieć ma numer 0, oznacza to, że cały adres dotyczy tylko sieci lokalnej. Ten rodzaj adresowania jest używany często przez ICMP (*ang. Internet Control Message Protocol*), jeden z podprotokołów protokołu IP odpowiedzialnych za sterowanie siecią Internet. Jeśli w części określającej sieć znajdują się same jedynki (czyli liczba dziesiętna 255), adres dotyczy pakietu rozgłoszeniowego, który jest rozsyłany do konkretnego komputera w sieci lokalnej. Jeśli same jedynki znajdują się w części określającej numer komputera, adres dotyczy pakietu rozgłoszeniowego, który jest rozsyłany do wszystkich stanowisk w sieci wskazanej przez pozostałą część adresu i we wszystkich podsieciach tej sieci. Jeśli adres składa się z samych jedynek (co daje 255.255.255.255) mamy do czynienia z pakietem rozgłoszeniowym, który jest rozsyłany do wszystkich stanowisk w sieci (i w podsieciach) lokalnej.

Klasy adresów

W adresie klasy A (rysunek 6.2) najbardziej znaczący bit (czyli ten z lewej strony) jest zawsze zerem, a pozostałe siedem bitów tego bajtu określają numer sieci. Pozostałe 24 bity wskazują na adres stanowiska w sieci. W ten sposób można zaadresować 128 sieci i ponad 16 mln komputerów.

W adresie klasy A jeden bajt określa numer sieci, a trzy numer komputera. Adresowanie typu A jest używane przez nieliczne, duże sieci komercyjne, np. przez sieć MILNET. Adresem tej klasy jest np.11.255.211.45.

W adresie klasy B dwa najbardziej znaczące bity przyjmują wartość 10 (binarnie). Kolejne 14 bitów określa numer sieci, a pozostałe 16 numer komputera. Pozwala to zaadresować 16 864 sieci i ponad 64 000 komputerów. Przekładając to na bajty, numer sieci w tej klasie zawiera się w przedziale 128.0-191.255. W tej klasie zarówno numer sieci, jak i komputera są określane przez dwa bajty (z tym, że numer sieci jest skrócony o dwa bity). Przykładowy numer tej klasy to 128.127.34.76.

W adresie klasy C trzy najbardziej znaczące bity muszą przyjąć wartość 110 (notacja binarna). Kolejne 21 bitów określa numer sieci, a pozostałe 8 numer komputera. Pozwala to zaadresować ponad 2 mln sieci i 254 mln komputerów. Numer sieci zawiera się, więc w przedziale 192.0.0-223.255.255. Pierwsze trzy bajty określają numer sieci, a jeden - numer komputera.

I wreszcie adres klasy D, w którym połowa pierwszego bajtu (a więc cztery najbardziej znaczące bity) przyjmuje wartość 1110. Pozostałe 28 bitów są używane do adresowania komputerów w trybie multicast (dokładnie opisany w RFC-1112).

Istnieją też adresy klasy E, w których cztery najbardziej znaczące bity są jedynkami (1111), adresy te są zarezerwowane do użytku NIC.

Podsieci w Sieci Internet

Organizacje używające adresowania klasy A i B (rzadziej klasy C) dzielą często całą sieć komputerową na mniejsze części, zwane podsieciami (rysunek 6.3). Każda z podsieci może reprezentować jedną z fizycznych część sieci (np. budynek czy piętro) lub obsługiwać konkretną grupę użytkowników (np. oddział czy biuro). Podsieci te mogą pracować w różnych standardach, np. Ethernet, Token Ring czy X.25, połączonych w jeden organizm systemem routerów. Decydując się na podzielenie sieci (na podsieci) należy zdecydować, jaką część adresu Internet (w części określającej numer komputera**,** a nie sieci) przeznaczymy na numer podsieci. Wydzielamy, więc w tym celu określoną liczbę bitów, które będą wskazywać na jedną z podsieci.

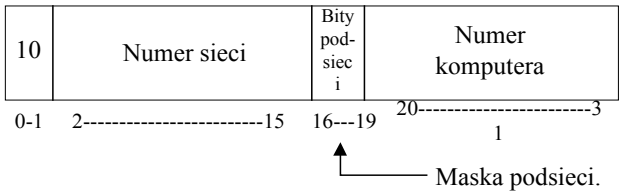
Na przykład w adresie klasy B numer sieci określają dwa najbardziej znaczące bajty (czyli 16 bitów), a numer komputera dwa najmniej znaczące (te z prawej strony). Jeśli więc zdecydujemy się na wycięcie z tych 16 bitów określających numer komputera czterech bitów na numer podsieci, to do adresowania komputerów w sieci zostanie nam 12 bitów. Pozwala to na przyznanie adresów 4096 komputerom w każdej z podsieci, co w zasadzie jest liczbą wystarczającą. Cztery bity podsieci pozwalają nam zaadresować 16 podsieci (od 0 do 15).

Bity podsieci są często używane do zamaskowania przed światem zewnętrznym skomplikowanej struktury sieci lokalnych. Komputer z zewnątrz nie "widzi" bowiem podsieci. Dla niego w adresie klasy B wszystkie 16 bitów określają numer komputera w danej sieci lokalnej, niezależnie od tego, ile bitów administrator wyznaczył na numerowanie podsieci. Wydzielenie podsieci wiąże się z utworzeniem tzw. maski podsieci**,** w której bity określające adres komputera są zerami, a bity określające numer sieci i podsieci jedynkami. I tak na przykład po wydzieleniu czterech bitów na adresowanie podsieci w adresie klasy B maska podsieci przyjmuje wartość 255.255.240.0.

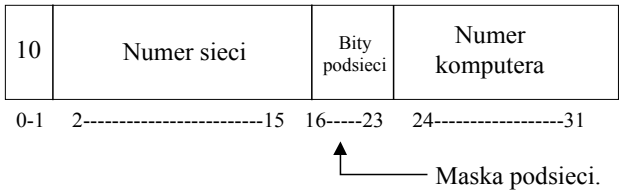
Program obsługujący ruch pakietów z w sieci lokalnej używa maski do sprawdzenia, czy obie stacje (wysyłająca i odbierająca) znajdują się w tej samej podsieci. Maska jest więc przykładana zarówno do numeru stacji wysyłającej pakiet, jak i do numeru stacji przeznaczenia. Jeśli jest to ta sama podsieć, pakiet jest wysyłany normalnie w daną podsieć (oczywiście, po wcześniejszym poddaniu adresu Internet konwersji na fizyczny numer stacji w sieci). Numer ten jest wyliczany przez protokół ARP, przyporządkowujący każdemu adresowi Internet w danej podsieci fizyczny adres karty sieciowej zainstalowanej w tym komputerze. W sieciach standardu Ethernet jest to adres o długości 48 bitów, reprezentowany przez 12 liczb heksadecymalnych**,** np. 0243a6234cde. Jeśli jednak analiza wykazuje, że jest to inna podsieć, pakiet jest kierowany do właściwego routera, który przerzuca go do właściwej podsieci.

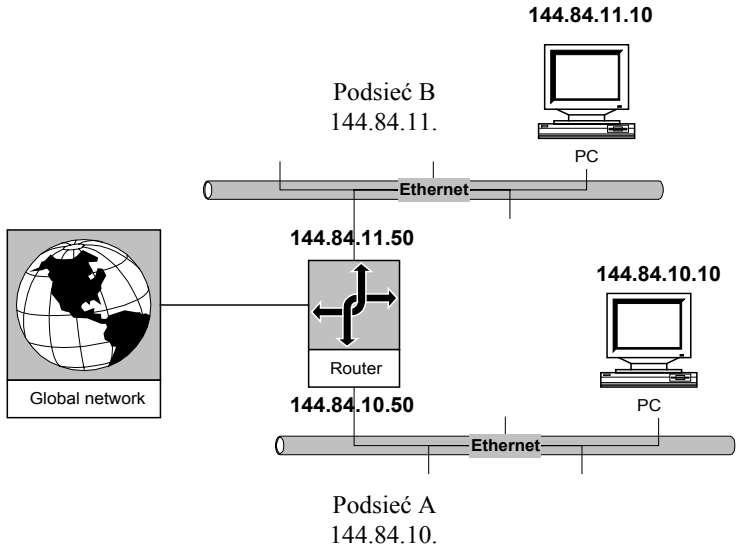
Posłużmy się tu przykładem. Załóżmy, że komputery w naszej sieci mają przyznane adresy zgodnie z notacją klasy B, a organizacja NIC zadecydowała, że sieć będzie nosić numer 144.84. Pozostała część adresu (a więc 16 bitów, czyli dwa bajty) będzie identyfikować poszczególne komputery dołączone do tej sieci.

Adres klasy B z maską podsieci.
Cztery bity podsieci.



Adres klasy B z maską podsieci.
Osiem bitów podsieci.





Osiem bitów podsieci. Maska Podsieci 255.255.255.0

Rysunek 6.3. Maska podsieci dla adresu klasy B

Każdy komputer w naszej sieci będzie, więc nosić numer 144.84.x.y, gdzie 144.84 to numer sieci, a x.y to numer komputera w tej sieci.

Sieć ma stosunkowo prostą architekturę i składa się z dwóch nitek (A i B), obsługujących dwa oddzielne budynki. Nitki te są dołączone do routera, który łączy nasz zakład ze światem zewnętrznym. Aby sprawa była jeszcze prostsza, do każdej z tych nitek jest dołączony tylko jeden komputer. Komputer dołączony do sieci A ma numer 144.84.10.10, a do sieci B - 144.84.11.10. Aby uprościć zadanie zarządzania siecią komputerową, decydujemy się na podzielenie jej na dwie podsieci. W tym celu dzielimy szesnaście bitów określających adres komputera w sieci na dwie równe części. Najmniej znaczące osiem bitów (a więc y) określa wtedy adres komputera w podsieci x. Konfigurując pakiety komunikacyjne, instalowane w poszczególnych komputerach i w routerze, wpisujemy wartość maski podsieci 255.255.255.0 (normalnie maska podsieci

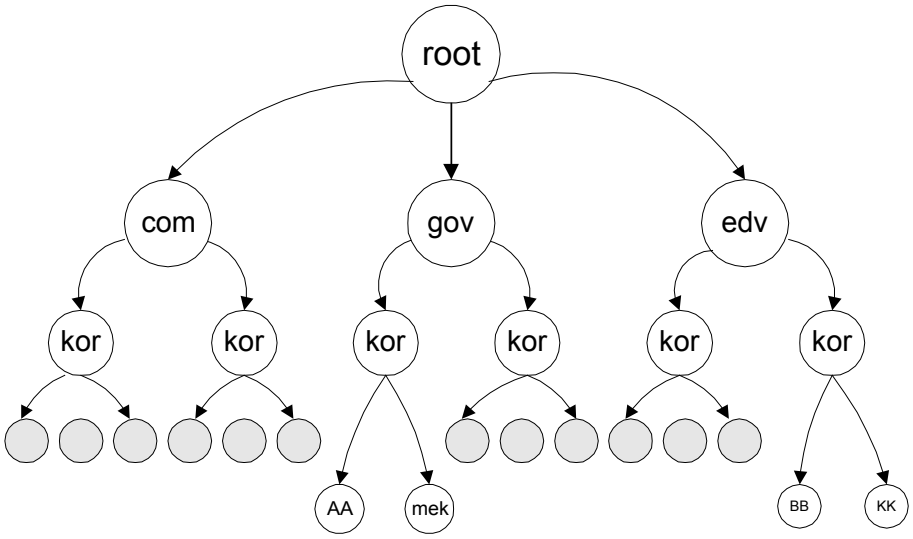
przyjęłaby wartość 255.255.0.0), a w miejsce liczby bitów podsieci wstawiamy wartość 8.

Dla świata zewnętrznego nasza sieć LAN nosi dalej numer 144.84, a dwa pracujące w niej komputery mają przyznane numery 10.10 i 11.10. Dla nas jednak numer 144.84.10.10 znaczy, że komputer numer 10 pracuje w podsieci 10 (w sieci 144.84),a numer 144.84.11.10, że komputer 10 pracuje w podsieci 11 (w sieci 144.84).

W każdej chwili sieć LAN można rozbudować o kolejne segmenty, przyznając im następne numery podsieci (np. 144.84.12, 144.84.13 itd.). Proszę zwrócić uwagę, że dla świata zewnętrznego sieć ta będzie cały czas nosić numer 144.84, a numery 10.y, 11.y, 12.y i 13.y identyfikują cztery stanowiska pracujące w jednej sieci 144.84. To, że sieć ta jest podzielona na dowolną liczbę podsieci wie tylko nadzorca zarządzający pracą danej sieci LAN (no i oczywiście oprogramowanie komunikacyjne zawiadujące ruchem pakietów w tej sieci).

6.3 Struktura drzewa DNS

Jak wiadomo, wszystkie komputery w sieci Internet komunikują się między sobą przy użyciu numerów IP Każdy taki numer ma postać czterech liczb dziesiętnych (od 0 do 255) oddzielonych kropką. Jeśli komputer A chce odczytać jakiś plik z komputera B (np. przy użyciu aplikacji FTP), to można to zrobić nie używając wcale nazw tych komputerów Wystarczy w poleceniach programu FTP wpisywać numer komputera B, a tak zaadresowany pakiet dotrze do tego komputera. Następnie komputer B odczyta numer IP komputera A i prześle do niego stosowny plik.



Rysunek 6.4 Struktura drzewa DNS

Cała sieć Internet może pracować bez przeszkód posługując się tylko numerami IP. Dotyczy to każdej bez wyjątku aplikacji (oprócz E-mail) uruchamianej w środowisku sieci Internet. Nazwy komputerów wymyślono wyłącznie po to, aby ułatwić życie osobom korzystającym z usług tej sieci. Dużo trudniej jest przecież zapamiętać numery komputerów niż przypisane im nazwy nie mówiąc o tym, że bardziej naturalne jest komunikowanie się z komputerem aa.rel.edu.pl niż z komputerem 145.87.32.44. Dlatego każdy komputer (a co za tym idzie każda sieć) ma w Internecie swoją nazwę.

Przekładaniem nazw przyznanych komputerom na przypisane im numery IP zajmuje się w sieci Internet (rysunek 6.4) zorganizowany w sposób hierarchiczny; rozproszony system serwerów o nazwie DNS (*ang. Domain Name Server*). Może ktoś pomyśleć, że wystarczyłoby uruchomić jeden silny serwer, który zarządzałby dużą bazą danych, zawierającą wszystkie nazwy i odpowiadające im numery IP.

Jest to jednak absolutnie niemożliwe. Należy pamiętać, że Internet jest siecią rozległą, komunikujące się ze sobą komputery mogą być zlokalizowane (i często są) na różnych kontynentach. Każdy z inicjujących sesję łączności komputerów musiałby łączyć się z tym odległym serwerem, w celu przetłumaczenia nazwy jakiegoś komputera na numer IP a przecież wiadomo, jak olbrzymia liczba komputerów pracuje w sieci Internet. Nie mam danych dotyczących innych rodzajów sieci LAN, ale jeśli chodzi o Ethernet, to na świecie pracuje już 500 tysięcy sieci tego standardu (którym przypisano stosowne numery IP). Jeśli założymy; że w jednej takiej sieci pracuje przeciętnie 10 komputerów to otrzymamy liczbę 5 milionów stanowisk pracy. Takiego ruchu pakietów nic wytrzymałaby żadna sieć, nie mówiąc już o tym, że jeden serwer nazw nie mógłby świadczyć jednocześnie swych usług tysiącom zgłaszających się do niego klientów.

Jedynym sensownym rozwiązaniem było więc podzielenie sieci Internet na poszczególne domeny, w ramach których pracują serwery nazw świadczące swe usługi zarówno poszczególnym stanowiskom pracy, jak i innym serwerom nazw (np. z innych domen). Ważne jest to, że domeny te są zorganizowane w strukturę hierarchiczną (drzewiastą), podobną do struktury katalogów w obrębie jednego komputera.

W każdej sieci LAN dołączonej do Internetu pracuje więc serwer DNS, do którego zadań należy podawanie numeru IP odpowiadającego nazwie komputera. W ten sposób na świecie pracują dziesiątki tysięcy serwerów DNS, które świadczą sobie wzajemnie usługi.

Nazwy przydzielane komputerom składają się z dowolnej liczby wyrażeń alfanumerycznych (cyfr i liter), oddzielonych kropką (np. BB.lec.edu.pl). W przypadku podania pełnej nazwy komputera FQND (*ang. Fully Qualified Name Domain*) wyrażenie z lewej strony jest nazwą komputera, a pozostałe są kolejnymi domenami, aż do samego wierzchołka struktury domen.

Wyobraźmy sobie sytuację, że chcemy się połączyć z komputerem o nazwie BB.lec.edu.pl, gdzie BB jest nazwą komputera, lec nazwą sieci, a edu.pl to nazwy kolejnych domen. Nazwa naszego komputera brzmi AA.rex.govpl. (AA - nazwa komputera, rex - nazwa sieci, gov pl - nazwy domen). Oprogramowanie sieciowe zainstalowane na naszym komputerze stwierdza na początku, że w dostępnych mu lokalnych tablicach (np. w pliku hosts.txt, jeśli pracujemy pod systemem DOS, lub w pliku usr/tmp/named dump.db, jeśli pracujemy pod Unixem) nie ma nazwy komputera BB. lec.edu.pl.

Program odczytuje, więc z pliku konfiguracyjnego oprogramowania sieciowego numer IP przypisany serwerowi DNS pracującemu w danej sieci LAN i wysyła do niego polecenie: podaj mi numer IP przypisany komputerowi BB.lec.edu.pl. Serwer DNS stwierdza, że w tablicach nic ma komputera o takiej nazwie (chyba że komunikowaliśmy się już wcześniej z tym komputerem i lokalny DNS zapisał to w tworzonych *ad hoc* tablicach). Lokalny DNS komunikuje się więc z serwerem DNS zarządzającym domeną lec.edu.pl lub z innym serwerem, który przepytuje kolejne serwery umieszczone na wyższych szczeblach hierarchicznej drabiny serwerów DNS itd., aż któryś z nich dotrze do serwera zarządzającego nazwami w domenie lec.edu.pl.

Serwer ten (noszący np. nazwę xx.lec.edu.pl) odpowiada nam - komputer BB.lec.edu.pl ma przypisany numer 193.54.11.22.

Jak więc widać, system serwerów DNS jest właściwie podzieloną na wiele partycji, olbrzymią, rozproszoną bazą danych, składającą się z mniejszych, współpracujących ze sobą, lokalnych baz. Na samym szczycie drzewa DNS znajdują się domeny grupujące komputery określonego rodzaju. Ich nazwy są już narzucone z góry przez NIC. Chodzi tu o kraje (.pl, .gb, .nor itd.) czy takie domeny jak: .gov (instytucje rządowe), .edu (szkolnictwo), .com (przemysł, handel, biznes) i .mil (wojskowość). Jeśli chodzi o nazwy domen niższego poziomu i nazwy pracujących w nich komputerów to ograniczeń takich nie ma i administrator danej sieci LAN czy organizacji może operować dowolnymi nazwami.

Pakiety współpracy z siecią Internet (pracujące pod różnymi systemami operacyjnymi) są wyposażane w aplikacje, które na życzenie użytkownika komunikują się z serwerami systemu DNS i podają numer IP komputera. W popularnym pakiecie działającym na komputerach PC (PC/TCP) jest to program host. Wystarczy wtedy napisać host <nazwa komputera> (np. host BB.lec.edu.pl), a aplikacja wypisze nam na ekranie adres odległego stanowiska pracy (BB.lec.edu.pl = 193.54.11.22). Na komputerach pracujących pod systemem Unix podobną usługę oferuje program nslookup.

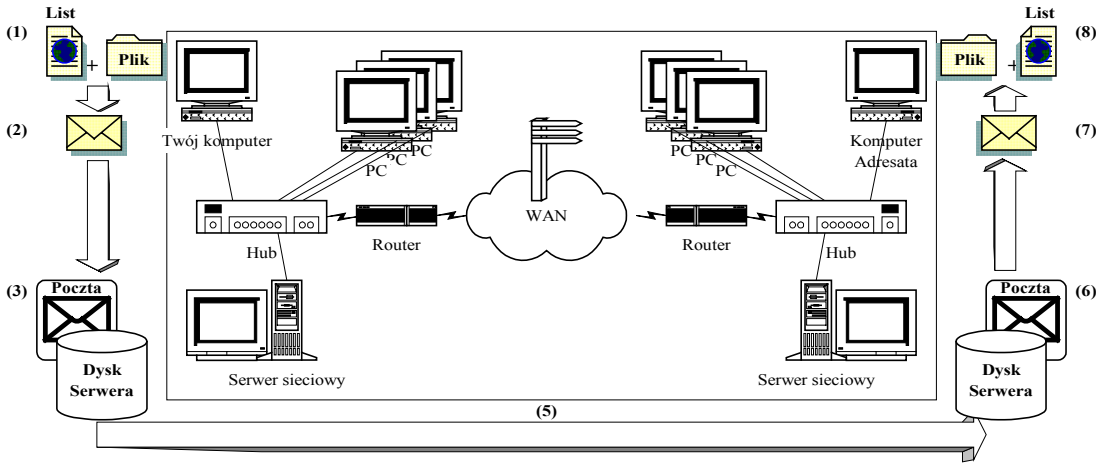
6.4 Usługi w sieci Internet

Poniżej przedstawiono kilka usług oferowanych przez sieć Internet. Usługi można podzielić na następujące kategorie:

- poczta elektroniczna (e-mail) - poczty można używać do korespondowania ze znajomymi, partnerami zawodowymi, można wysłać też wiadomość prezydentowi USA (*president@whitehouse.gov*), można zaprenumerować serwisy wiadomości lub przeszukiwać bazy danych.
- listy dyskusyjne - Internet jest miejscem, gdzie wielu ludzi wymienia swoje poglądy.
- uruchamianie programów na innych komputerach - można uruchamiać programy, które na posiadanym aktualnie sprzęcie nie działają, lub których po prostu nie ma potrzeby lub możliwości kopiowania na swój komputer.
- przenoszenie plików - ściągać można dowolne udostępnione pliki - zdjęcia astronomiczne, dane pogodowe, tekst, grafikę, animację, dźwięk, programy, sterowniki i w ogóle wszystko co można zapisać na dysku.
- poszukiwanie plików i przeglądanie baz danych - w Internecie istnieje kilka systemów umożliwiających przeglądanie tysięcy komputerów, ich plików i baz danych.
- gry i rozmowy - można rozmawiać z ludźmi na całym świecie (to co jest napisane jest natychmiast widoczne u wszystkich zainteresowanych), można uczestniczyć w grach RPG lub przyłączyć się do gry symulacyjnej.
- przeglądanie stron WWW (*ang. Surf till you drop* – żeglowanie po sieci Internet). Podróżować po internetowej cyberprzestrzeni można za pomocą różnych narzędzi; największą popularność zdobyła Światowa Pajęczyna WWW (*ang. World Wide Web*). Pajęczyna zawiera miliony stron, z których każda zawiera jakieś informacje oraz powiązania (linki) do innych stron.

Poczta elektroniczna

Działanie poczty elektronicznej opiera się na zasadzie składuj i prześlij dalej (*ang. store and forward*). Przedstawia to rysunek 6.5.



Rysunek 6.5 Przesyłanie wiadomości e-mail w sieci Internet

Oznacza to, że wiadomość jest wysyłana przez nadawcę do systemu składowania, skąd, gdy jest już gotowa, przekazywana jest do adresata. Zaletą tego rozwiązania jest fakt, że adresat nie musi być dostępny podczas nadawania wiadomości. Zaś droga, jaką przebywa wiadomość, zależy od aktualnego stanu obciążenia sieci.

Internetowa poczta elektroniczna opiera się na standardzie SMTP (*ang. Simple Mail Transfer Protocol*), który jest jednym ze składników IP. Każda przesyłka składa się z dwóch części: nagłówka oraz tekstu. Nagłówek w najprostszej postaci zawiera:

- From - od kogo pochodzi wiadomość;
- To - dane adresata;
- Date - data i czas wysłania;
- Subject - temat wiadomości.

Dodatkowo nagłówek może zawierać informacje na temat trasy przesyłki, identyfikatora przesyłki i inne. Przesyłki można wysyłać zarówno do jednego adresata jak i do wielu naraz.

Ponieważ pocztą można również wysyłać pliki binarne (programy, grafikę itp.), druga część przesyłki składa się z tekstu, część binarną należy przekonwertować do postaci tekstowej (program uuencode). Następnie przekodowany plik dołączany jest do wiadomości. Adresat po otrzymaniu wiadomości może przekonwertować plik z powrotem na postać binarną poleceniem uudecode.

Obecnie istnieje standard, który automatycznie dokonuje odpowiednich konwersji i nie trzeba się troszczyć o kodowanie i dekodowanie plików. MIME (*ang. Multipurpose Internet Mail Extensions*) redukuje niezbędne czynności przy wysyłaniu plików nietekstowych do dołączenia danego pliku do przesyłki i wysłaniu jej. Większość używanych programów pocztowych współpracuje ze standardem MIME. Programy pocztowe posiadają poza tym wiele innych ułatwień jak np. książki adresowe, szyfrowanie wiadomości lub zakładanie folderów dla poczty od różnych nadawców.

Listy dyskusyjne

Korzystając z listy dyskusyjnej otrzymujemy wszystkie listy jakie zostały do niej wysłane przez jej członków; podobnie nasze listy docierają do wszystkich z listy

dyskusyjnej. Lista dyskusyjna może być ograniczona lub nie. W listach dyskusyjnych wszystkie listy są filtrowane przez osobę lub grupę osób w celu upewnienia się czy są one odpowiednie dla danej listy.
Zapisywanie się do listy polega na wykonaniu 3 czynności:
- ustalenie adresu subskrypcyjnego;
- zorientowanie się, czy kontaktujemy się z programem czy też z człowiekiem;
- napisanie prośby i wysłanie jej pod adres subskrypcyjny.

Wykaz list dyskusyjnych można aktualnie otrzymać po wysłaniu przesyłki pod adres *listserv@bitnic.bitnet* z tekstem list global lub przekopiować pliki o nazwach *part01,part02* z *rtfm.mit.edu* z katalogu */pub/usenet-by-group/news.answers/mail/mailing-lists* korzystając z FTP.

Telnet

Telnet jest programem, który umożliwia połączenie się ze zdalnym komputerem (serwerem telnetowym) i co za tym idzie korzystanie z jego zasobów sprzętowych i programowych (np. gdy istnieje potrzeba uruchomienia programu wymagającego bardzo dużo pamięci operacyjnej).

Telnet umożliwia korzystanie z komputera zdalnego tak, jakby był on komputerem lokalnym. Po nawiązaniu połączenia i ustaleniu strategii komunikacji pomiędzy klientem i serwerem uruchamiany jest program *login*, po czym następuje normalna sesja użytkownika (na komputerze zdalnym). Komputer lokalny przesyła informacje wprowadzane przez użytkownika do komputera zdalnego jednym z dwóch sposobów: w trybie przesyłania całych linii (*line mode*) lub w trybie znakowym (*character mode*).

W wielu przypadkach użytkownik pytany jest o rodzaj emulacji terminala - najbardziej popularnym typem jest VT100. Dzięki telnetowi można łączyć się z serwerami, które pracują pod różnymi systemami operacyjnymi, na różnych platformach sprzętowych np. Amiga, DEC, IBM, HP albo MacIntosh. Oprócz programu *telnet* istnieją bardziej przyjazne dla użytkownika programy np. Gopher lub Hytelnet, który znajduje się pod adresem *ftp.usask.ca* w katalogu */pub/hytelnet.*

File Transfer Protocol

FTP pozwala na przenoszenie plików pomiędzy dowolnymi komputerami włączonymi do Internetu. Przenosić można dowolny udostępniony plik bez względu na to, czy jest to plik tekstowy, czy program lub grafika. Dostępne są programy darmowe, czyli *freeware* (często wraz z kodem źródłowym) lub *shareware*, czyli niepełne wersje programów komercyjnych.
Korzystanie z FTP polega na :
- wystartowaniu FTP i połączeniu się ze zdalnym komputerem;
- zmianie katalogu na ten, w którym planuje się pracować;
- ustawieniu opcji transferu plików;
- przekopiowaniu plików na lokalny komputer z komputera zdalnego lub odwrotnie;
- zakończeniu sesji FTP.

Dzięki FTP setki tysięcy plików są dostępne dla każdego użytkownika. W sieci można znaleźć najnowsze sterowniki do kart lub np. opracowania na temat lotnictwa z czasów I Wojny Światowej.

Przeszukiwanie sieci

Internet stanowi tak bogate źródło najprzeróżniejszych informacji, że jedynymi problemami w ich zdobyciu stają się często:
- brak informacji na temat ich lokalizacji;
- nadmiar informacji na temat ich lokalizacji.

Jednym ze starszych systemów służących do znajdywania plików jest Archie. Program wyszukuje tekst zawarty w nazwach plików i katalogów (np. można się domyśleć, że pliki graficzne będą posiadały rozszerzenie - *.jpg). Archie jest kolekcją wielu serwerów, które mają wydzielony swój obszar kontrolowania i tworzą własną bazę danych na temat plików znajdujących się na tysiącu serwerach. Archie jest systemem opartym na architekturze klient/serwer. Klient może pracować z domniemanym lub wybranym serwerem Archie z dowolnego komputera w sieci.

Inne często wykorzystywane Serwery - zawierające informacje na dany temat, pliki, wskazania na inne serwery zawierające podobne informacje - to Yahoo, AltaVista, Infoseek i inne. Dostępne są one pod nazwą domeny www.yahoo.com , www.altawista.com itd

World Wide Web WWW

WWW zostało wymyślone w 1990 roku w Genewie. Ideą twórców było stworzenie narzędzia, które maksymalnie ułatwiłoby poruszanie się po sieci. Fundamentem WWW jest *hipertekst*, który zawiera oprócz zwykłego tekstu słowa kluczowe, które są powiązane z innymi dokumentami hipertekstowymi, tzn. powodują wyświetlanie tych dokumentów (stron WWW).

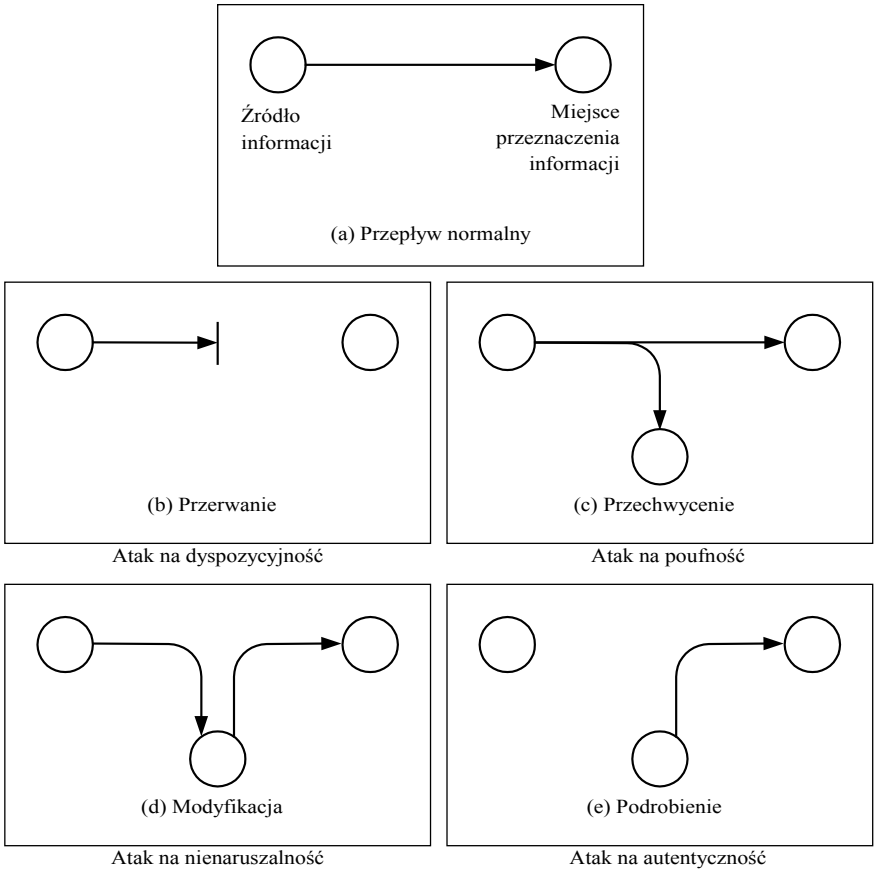
Do zalet WWW należy zaliczyć:
- nieliniowość - przejście do określonego dokumentu lub katalogu następuje natychmiast, bez uwidaczniania hierarchicznej struktury katalogów czy nazw serwerów;
- forma graficzna - dokument może zawierać obrazki, animacje, różne typy czcionek, przełączniki itp;
- interakcyjność - wiele dokumentów pozwala na wprowadzania własnego tekstu, wypełnianie formularzy, uruchamianie programów itp;
- uniwersalność - za pośrednictwem dokumentu można otworzyć sesję telnet, przeszukiwać bazy danych Archie lub korzystać z Usenetu.

Korzystanie z WWW umożliwiają przeglądarki (Internet Eksplorer, Netscape Navigator, Mosaic, Eudora). Większość z nich można za darmo otrzymać za pośrednictwem Internetu np. z Serwera sunsite.icm.edu.pl. albo zakupić wraz z egzemplarzem czasopisma komputerowego (np. chip i inne). Albo też zastać na swoim komputerze po zainstalowaniu systemu Windows 95, NT. Można również użyć w tym celu MS Word po uprzednim zainstalowaniu *Internet Assistant*.

W przypadku zupełnego braku przeglądarki można skorzystać z programu - przeglądarki pracującej w trybie liniowym za pomocą telnetu: *$telnet www0.cern.ch.*

7 Bezpieczeństwo w sieciach teleinformatycznych

Każdego dnia przybywa około 20 000 nowych komputerów podłączonych do sieci Internet. Ta największa publiczna sieć komputerowa przyciąga coraz szersze rzesze użytkowników, oferując im bogate zbiory informacyjne, grupy dyskusyjne, wymianę poczty elektronicznej, gry sieciowe a nawet możliwości prowadzenia rozmów "*on line*". Opierając się na danych statystycznych sporządzonych przez Network Wizards (*http://www.nw.com*) można przypuszczać, iż przed zakończeniem naszego stulecia Internet obejmie swoim zasięgiem ponad 50 milionów komputerów. Wraz ze wzrostem liczby użytkowników Internetu rośnie ryzyko utraty prywatności lokalnych sieci komputerowych.

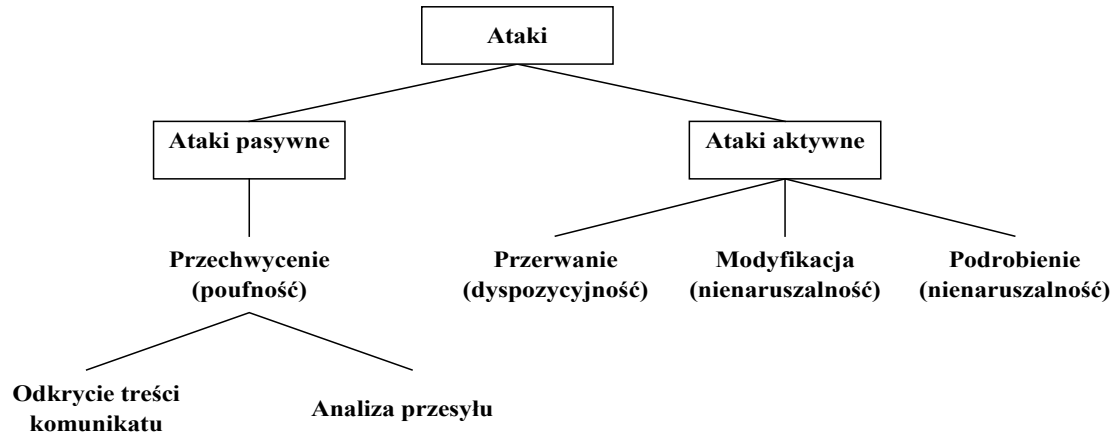


Rysunek 7.1 Klasyfikacja zagrożeń

Najbardziej skutecznym sposobem zniwelowania potencjalnych zagrożeń bezpieczeństwa (rysunek 7.1), wynikających z podłączenia do sieci publicznej, jest fizyczne odseparowanie wszystkich komputerów wspomagających realizację istotnych zadań organizacji i przechowujących jej strategiczne informacje. W praktyce, oznacza to kompleksową przebudowę fizycznej infrastruktury systemu informatycznego, co w dużej większości przypadków pociąga za sobą poważne wydatki finansowe. Rozwiązaniem tego problemu jest zastosowanie oprogramowania firewall (ściana ognia, gateway ochronny) dedykowanego do ochrony systemu lokalnego przed ingerencją zewnętrzną.

7.1 Zagrożenia

Aby zbudować skuteczny system zabezpieczeń trzeba wiedzieć, przed czym się bronić, jakie są rodzaje ataków (rysunek 7.2).



Rysunek 7.2 Klasyfikacja ataków

Zasadniczo, oprogramowanie firewall nie zapewnia ochrony systemu przed użytkownikami lokalnymi można, więc ograniczyć rozważania do zagadnienia zagrożeń zewnętrznych, zakładając optymistycznie, że wszystkie osoby posiadające lokalny dostęp do systemu są upoważnione do wykonywanych przez nie operacji. Nie znaczy to jednak, że nie mamy możliwości zbudowania systemu wewnętrznych zabezpieczeń.

Telnet

Najpowszechniej praktykowaną metodą uzyskiwania dostępu do odległego systemu jest wykonywanie zdalnego logowania Telnet (ang. *Network Terminal Protocol*), przeprowadzanego najczęściej na bazie łączności modemowej "dial-up". Warunkiem wykonania pomyślnego logowania na odległym komputerze jest znajomość identyfikatora i hasła użytkownika, który jest do tego upoważniony. Uzyskanie identyfikatora z reguły sprowadza się do zdobycia adresu e-mail dowolnego użytkownika tego systemu. Hasła użytkowników mogą być pozyskane drogą zgadywania, przechwytywania lub rozszyfrowania pliku zawierającego hasła użytkowników systemu. Co ciekawe, sama aplikacja Telnet nie stanowi zagrożenia - to przyjęty system kontroli tożsamości jest słaby. Statystyki podają, iż duża większość użytkowników jako hasła dostępu do konta przyjmuje łatwe do zapamiętania słowa (np. imiona, nazwy miejscowości), które w równie łatwy sposób mogą być odgadnięte przez cierpliwego włamywacza ("hackera").

Nasłuch

Przechwytywanie hasła może odbywać się za pośrednictwem ukrytego w systemie programu, który odbiera wpisywane przez użytkownika dane (np. fałszywy program *login*) lub poprzez prowadzenie "nasłuchiwania sieci" (ang. *sniffing*) wykonywanego w trakcie zdalnego logowania legalnego użytkownika. "Sniffing" odbywa się za pośrednictwem urządzeń podsłuchowych, podłączonych do sieci na drodze transmisji danych. W najprostszym przypadku może to być zmodyfikowana karta sieciowa umożliwiająca selektywne przechwytywanie pakietów.

Sniffing to bardzo poważny problem, który nie ogranicza się wyłącznie do przechwytywania hasła - w przypadku prowadzenia nieszyfrowanej transmisji danych "nasłuchiwanie sieci" może prowadzić do całkowitej utraty poufności przesyłanych informacji. Niestety, nie ma skutecznych narzędzi przeciwdziałania tej technice - dostępne programy monitorujące pracę sieci komputerowej nie gwarantują wykrycia dobrze zamaskowanego urządzenia podsłuchowego. Nawet zastosowanie łącza światłowodowego nie zapewnia pełnej tajności transmitowanych informacji (więcej informacji można uzyskać w Internecie pod adresem: http://www.cert.org).

Złośliwe programy

Pewne niebezpieczeństwo stanowi usługa transferu plików FTP (*ang. File Transfer Protocol*). Wykorzystując niewłaściwie administrowany serwer FTP, użytkownik Internetu może wejść w posiadanie ważnych informacji, przechowywanych w systemie plików komputera. Bardzo groźnym zjawiskiem jest wykorzystanie FTP do rozprowadzania tzw. "złośliwych programów" (*ang. malicious programs*).
W gronie tych aplikacji możemy wyróżnić następujące programy złośliwe.

- **Wirus** (*ang. virus*) - program dopisujący się do innego programu, który atakuje system w trakcie uruchomienia swojego "żywiciela";
- **Bakteria** (*ang. bacteria*), "królik" (*ang. rabbit*) - program wielokrotnie kopiujący i uruchamiający swój własny kod źródłowy celem pełnego zagarnięcia zasobów komputera (czasu procesora, pamięci operacyjnej, przestrzeni dyskowej) i doprowadzenia do upadku systemu;
- **Koń trojański** (*ang. trojan horse*) - program, który udaje pracę innego legalnego programu, a w międzyczasie wykonuje szereg niepożądanych czynności (np. fałszywy program *login* kradnie hasło użytkownika);
- **Bomba czasowa** (*ang. time bomb*), "bomba logiczna" (ang. *logic bomb*) - fragment programu podejmujący działanie tylko w określonym czasie (np. dzień urodzin autora programu) lub w momencie spełnienia ustalonych warunków;
- **Robak** (*ang. worm*) - program, który powiela samego siebie, wykonuje ustalone czynności (najczęściej niekorzystne dla systemu) i próbuje przenieść się do innego komputera w sieci.

Z uwagi na właściwość samoprzenoszalności, "robak" wydaje się być najbardziej niebezpiecznym członkiem powyżej wymienionej grupy programów. Pierwszy atak "robaka" zarejestrowano w 1988 roku. Program napisany przez Roberta Morrisa przenosił się z komputera na komputer poprzez wykorzystywanie słabych punktów aplikacji SENDMAIL, FINGERD i RHOST.

Furtki i włazy

Inną kategorią zagrożeń są tzw. "furtki" (*ang. backdoors*) lub "włazy" (*ang. trapdoors*), które stanowią nieudokumentowane wejścia do legalnych programów. Niekiedy, programiści tworzą alternatywne wejście do aplikacji, aby ułatwić sobie proces testowania. "Furtką" do programu może być ciąg znaków lub nawet wciśnięcie odpowiedniej kombinacji klawiszy. W momencie odnalezienia "furtki" nieuprawniony użytkownik uzyskuje kontrolę na aplikacją.

SMTP i WWW

Omawiając niebezpieczeństwa związane z wykorzystaniem Internetu nie należy zapominać o dwóch najbardziej popularnych usługach - serwisie wymiany poczty elektronicznej SMTP (*ang. Simple Mail Transfer Protocol*) i serwisie informacyjnym WWW (*ang. World Wide Web*). Najsłabszą stroną systemu poczty elektronicznej Internetu okazał się program *sendmail*. W ostatnich latach odnotowano przypadki wykorzystania niedostatecznych zabezpieczeń tego programu do oszukiwania serwera SMTP, który poprzez błędną interpretację nadchodzących przesyłek, traktował je jako programy wykonywalne.

Próby rozszerzenia możliwości WWW (np. interfejs CGI, nowe elementy HTML), spowodowały powiększenie pola działania "hackerów". Administratorzy serwerów WWW często decydują się na korzystanie ze sprowadzonych z Internetu skryptów *CGI (ang. Common Gateway Interface*). Uruchamianie nieznanych aplikacji nieuchronnie wiąże się z podejmowaniem ryzyka, uzyskania odmiennego niż zakładano, rzeczywistego rezultatu działania programu. Ostatnie rozszerzenia języka opisu dokumentów hypertekstowych HTML (*ang. HiperText Markup Language*), zmierzają w kierunku wprowadzenia do WWW elementów bezpośredniej interakcji z użytkownikiem. Bez wątpienia najbardziej eleganckim rozwiązaniem jest wzbogacanie stron HTML o aplikacje napisane w języku Java. Warto jednak pamiętać, iż Java jest bardzo "młodym" językiem programowania, a zastosowany system bezpieczeństwa może okazać się nie w pełni skuteczny. Informacje na temat ryzyka wynikającego z uruchamiania sprowadzanych z Internetu programów Java można znaleźć pod adresem: http://www.cs.princeton.edu.

Spoofing

Chyba najgłośniej omawianą obecnie techniką oszukiwania zabezpieczeń systemów (w tym systemów chronionych przez niektóre "firewall") jest "spoofing". Określenie "spoofing" wywodzi się z dziedziny wojskowej i oznacza *przeciwdziałanie elektronicznym przeciwsystemom nieprzyjaciela poprzez nadawanie fałszywych informacji*. W odniesieniu do zagadnienia transmisji danych w sieci TCP/IP, "IP Source-Address Spoofing" oznacza proces przesyłania pakietów zawierających nieprawdziwy adres źródłowy (*ang. source address*), przez co komputer odbierający te pakiety błędnie identyfikuje ich nadawcę. Pierwszy poważny atak przeprowadzony z wykorzystaniem tej techniki został odnotowany 22 stycznia 1995 roku w USA.

Zakres przedstawionych powyżej potencjalnych zagrożeń, jakie należy uwzględnić podczas budowy polityki bezpieczeństwa, został świadomie ograniczony tylko do tych zagadnień, którym można przeciwdziałać poprzez "firewall". Nie ma potrzeby rozważać niebezpieczeństwa przechwytywania zainicjowanych połączeń sieciowych (*ang. connection hijacking*) czy rejestracji fal elektromagnetycznych, emitowanych przez drukarki, monitory komputerów czy przewody instalacji sieciowej, skoro "firewall" w niczym tu nie pomoże. Należy także pamiętać, iż wymienione zagrożenia obejmują tylko to, co do tej pory zostało wykryte i ujawnione publicznie.

7.2 Bezpieczeństwo WWW

Koncepcja współpracy z intersiecią bazuje na kombinacji technologii WWW i Java, stanowiących uniwersalny system dystrybucji aplikacji w środowisku sieci komputerowych. Serwis informacyjny World Wide Web funkcjonuje w oparciu o

protokół HTTP (*ang. HyperText Transfer Protocol*), który wraz z językiem HTML pozwala na efektywne rozprowadzanie informacji.

Serwery WWW udostępniają dane w formie dokumentów hipertekstowych. Dokument hipertekstowy jest zbiorem pojedynczych stron połączonych ze sobą odnośnikami (linkami). Każda ze stron jest zapisana w języku HTML i może zawierać tekst, elementy grafiki, dźwięku i animacji oraz aplikacje (w tym programy napisane w języku Java). Efektywność funkcjonowania WWW wynika z faktu, iż pojedyncze strony dokumentu hipertekstowego nie są przesyłane jako tradycyjne pliki graficzne, lecz w formie tekstu (opisu) w języku HTML, na podstawie, którego przeglądarka WWW (*ang. browser*) odtwarza wygląd dokumentu. Każda strona dokumentu hipertekstowego jest jednoznacznie identyfikowana w całym obszarze sieci Internet na podstawie unikalnego adresu URL (*ang. Uniform Resource Locator*) np. *http://www.wat.waw.pl/index.html*

Działanie WWW jest niewątpliwie bardzo wydajne, jednak w odniesieniu do zagadnień bezpieczeństwa pozostawia wiele do życzenia. HTTP i HTML nie zawierają żadnych wbudowanych mechanizmów pozwalających na utrzymywanie poufności, autentyczności i nienaruszalności przesyłanych informacji. Dodatkowa niedogodność wynika z samej istoty funkcjonowania protokołu HTTP, który zakłada, iż sesja komunikacyjna pomiędzy serwerem i przeglądarką WWW odnosi się jedynie do jednej strony HTML tzn. serwer WWW po udostępnieniu strony o określonym adresie URL niezwłocznie zamyka połączenie sieciowe z przeglądarką. Ze względów efektywności nie jest wskazane, aby negocjacje pomiędzy serwerem i przeglądarką dotyczące parametrów szyfrowania i uwierzytelniania przekazywanych danych były prowadzone dla każdej strony dokumentu hipertekstowego z osobna. Protokół HTTP pozwala jedynie na prowadzenie kontroli dostępu do poszczególnych stron WWW. Potwierdzenie tożsamości użytkownika odbywa się poprzez podanie danych identyfikacyjnych *username-password*, przekazywanych do serwera WWW w formie jawnej. Tak przesyłane informacje mogą zostać swobodnie odczytane w trakcie transmisji i wykorzystane przez osoby nieupoważnione. Aby zapewnić odpowiednią ochronę WWW należy zastosować dodatkowe środki zabezpieczające.

Secure Sockets Layer (Netscape Communications)

Jedną z najpoważniejszych propozycji jest technologia SSL (*ang. Secure Sockets Layer*)**,** opracowana przez *Netscape Communications*. SSL umożliwia szyfrowanie i uwierzytelnianie przekazywanych informacji oraz ustalanie prawdziwej tożsamości komunikujących się serwerów i przeglądarek WWW. Funkcjonowanie SSL odbywa się w oparciu o protokół transmisji połączeniowej TCP (Transport Control Protocol) i ogranicza się do zakresu warstwy transportowej modelu komunikacyjnego TCP/IP, co pozwala na zastosowanie tej technologii do ochrony innych usług Internetu np. FTP, Telnet, Mail. Specyfikacja SSL obejmuje dwa podstawowe protokoły:

SSL Handshake Protocol określa metody prowadzenia negocjacji pomiędzy serwerem i przeglądarką WWW, mające na celu ustalenie parametrów bezpiecznej sesji komunikacyjnej np. algorytmy szyfrowania danych, algorytmy sprawdzania autentyczności i integralności informacji, klucze szyfrowania.

SSL Record Protocol określa format przesyłanych pakietów danych w ramach chronionej sesji komunikacyjnej.

Wersja 3 specyfikacji SSL przewiduje stosowanie algorytmów szyfrowania DES, Triple-DES, IDEA, RC2 i RC4 wraz z jednokierunkową funkcją skrótu MD5 lub SHA oraz algorytmy RSA i DSS do tworzenia podpisów cyfrowych. W procesie negocjacji

kluczy szyfrowania, SSL używa algorytmu Diffiego-Hellmana. Serwery WWW wykorzystujące protokół SSL mogą prowadzić zarówno szyfrowane jak i jawne sesje komunikacyjne (zapytania SSL obsługiwane są na porcie 443, a nie na standardowym dla protokołu HTTP numerze portu 80). Zabezpieczone przez SSL strony dokumentu hipertekstowego posiadają odmienny format adresu URL - *https://*. Oprócz produktów firmy *Netscape Communications*, SSL doczekał się zastosowań w popularnych aplikacjach *Microsoft*: Internet Explorer 3.0 i Internet Information Server 3.0.

Private Communication Technology (Microsoft)

Opracowany wspólnie z *NetManage, Inc.* protokół PTC **(***ang. Private Communication Technology*) był odpowiedzią *Microsoft* na SSL, jednak z uwagi na fakt, iż najnowsze produkty tej firmy zawierają obok PCT również implementacje SSL, można przypuszczać, że *Microsoft* nie będzie rozwijał tej technologii w przyszłości.

Protokół S-HTTP (Enterprise Integration Technologies)

Innym rozwiązaniem, dedykowanym wyłącznie dla WWW, jest protokół S-HTTP (*ang. Secure HyperText Transfer Protocol*), opracowany przez Enterprise Integration Technologies i używany np. w serwerach firm *NCSA, Open Market, Apache, CERN, Spyglass* i *IBM*. S-HTTP jest w pełni zintegrowany z protokołem HTTP - ustalenia dotyczące ochrony przesyłanych stron HTML odbywają się z wykorzystaniem standardowych komunikatów HTTP. Specyfikacja S-HTTP zakłada, iż w procesie szyfrowania i uwierzytelniania informacji mogą zostać wykorzystane algorytmy kryptograficzne:

- do szyfrowania - DES, Triple-DES, IDEA, RC2, RC4 ()
- do podpisów cyfrowych oraz RSA, DSS, MD5, MD2 i SHA.

S-HTTP jest stosunkowo mało rozpowszechniony, ponieważ najbardziej popularne komercyjne przeglądarki WWW (Netscape Navigator, MS Internet Explorer) wykorzystują jednak SSL. S-HTTP został wdrożony praktycznie tylko w przeglądarce Mosaic (*NCSA, Spyglass*).

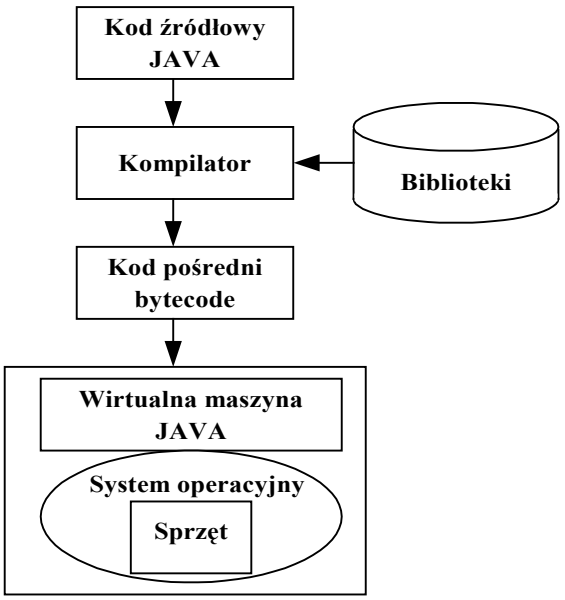
Protokół SET (MasterCard i Visa International)

W ostatnim czasie dużą popularność zyskuje możliwość prowadzenia transakcji finansowych za pośrednictwem sieci publicznych. Chęć dotarcia do większego grona klientów skłoniła wiele instytucji do rozszerzenia swojej działalności na obszar sieci Internet. W takiej sytuacji, oprócz standardowych mechanizmów ochrony informacji, wymagana jest niezawodna metoda określania tożsamości stron uczestniczących w transakcji oraz bezpieczny system obsługi kart kredytowych. Jednym z najczęściej używanych protokołów tej klasy zabezpieczeń jest SET (*ang. Secure Electronic Transaction*), opracowany przez MasterCard i Visa International, przy współudziale (między innymi) Verisign, IBM, Netscape i Microsoft.

7.3 Język programowania Java (SUN Microsystems)

Opracowany przez *SUN Microsystems,* język Java mimo, iż koncepcyjnie stworzony dużo wcześniej, oficjalnie pojawił się na rynku w maju 1995 roku. Popularność Java wynika wprost z dynamicznego rozwoju i rozpowszechnienia sieci Internet, a w szczególności rosnącego zainteresowania komercyjnym wykorzystaniem serwisu informacyjnego WWW. Java to nie tylko język, to także technologia

opracowana z myślą o zastosowaniach w otwartych, heterogenicznych środowiskach sieciowych, takich jak Internet (rysunek 7.3).

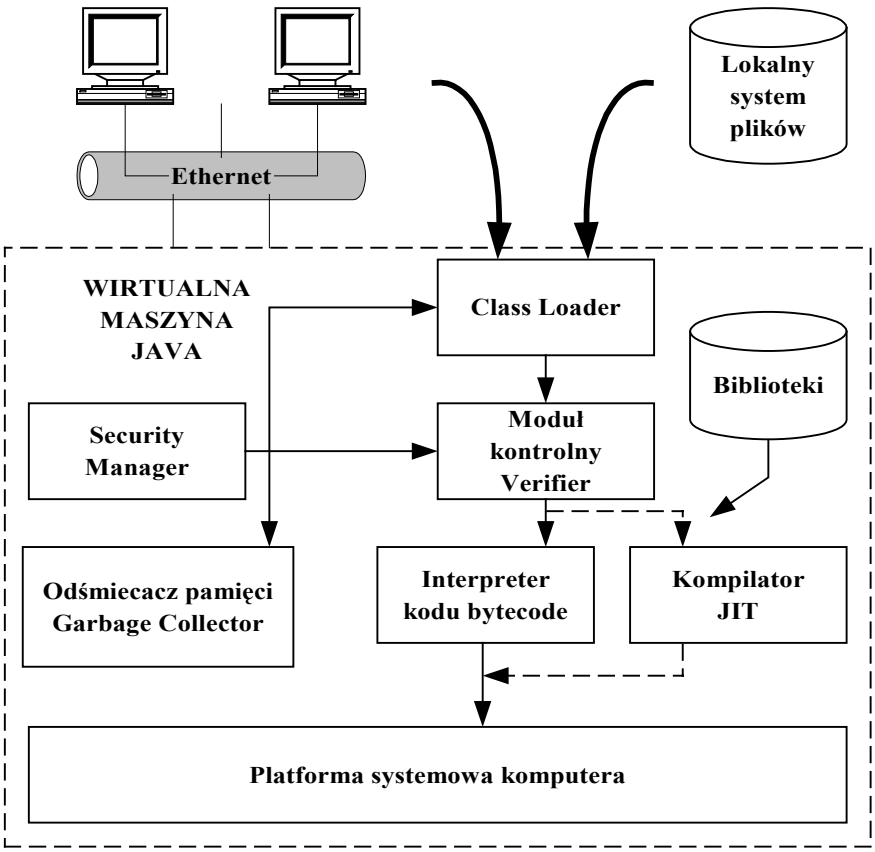


Rysunek 7.3 Koncepcja języka Java

Programy napisane w Java są niezależne od platformy wykonawczej (architektury sprzętowej i systemu operacyjnego) i mogą być uruchamiane na każdym komputerze, który został wyposażony w tzw. *"Wirtualną Maszynę Java"* (ang. *Java Virtual Machine* (JVM)). Java jest pełnowartościowym, obiektowym językiem programowania, łudząco przypominającym C++ (rysunek 7.4). Zasadnicza różnica pomiędzy tymi językami wynika z faktu, iż aplikacje Java są kompilowane do postaci kodu pośredniego *byte-code*, a nie do kodu maszynowego jak to ma miejsce w C++, czy w każdym innym, popularnym języku programowania. Kod pośredni zawiera instrukcje dla *Wirtualnej Maszyny Java.*

Najbardziej rozpowszechnioną formą wykorzystania tej technologii są aplety - niewielkie aplikacje "wbudowane" w dokumenty hipertekstowe WWW, znacząco wzbogacające HTML o elementy funkcjonalne związane np. z interakcyjnością, czy animacją.

Wykorzystanie apletów wzbudza wiele kontrowersji z uwagi na duże, potencjalne zagrożenie dla bezpieczeństwa. Kto może zagwarantować, że program sprowadzony z sieci publicznej w postaci wykonywalnej, nie okaże się "koniem trojańskim", który oprócz przewidywanego działania przeprowadzi szereg innych, niepożądanych czynności (np. sformatowania twardego dysku). Obawy te są w pełni uzasadnione w odniesieniu do aplikacji napisanych w Pascalu, C/C++, Adzie, czy w każdym innym popularnym języku programowania. W przypadku języka Java mamy do czynienia z bardzo ostrą polityką bezpieczeństwa zmierzającą do ochrony środowiska wykonawczego.



Rysunek 7.4 Struktura wirtualnej maszyny Java

Przyjęty model bezpieczeństwa odnosi się do specyfikacji języka, fazy kompilacji kodu źródłowego Java, a przede wszystkim do procesu uruchamiania programu w środowisku wirtualnej maszyny Java. Specyfikacja języka zwraca szczególną uwagę na prawidłowe zarządzanie pamięcią operacyjną. Brak typu wskaźnikowego znacznie obniża prawdopodobieństwo występowania błędów programu. Java świadomie odbiera programiście możliwość uzyskiwania bezpośredniego dostępu do pamięci operacyjnej. Zaimplementowany w JVM mechanizm "odśmiecania" pamięci (*ang. garbage collector*) dokonuje automatycznego zwolnienia niewykorzystywanych przez aplikację bloków pamięci. W procesie kompilacji prowadzona jest wnikliwa kontrola poprawności kodu źródłowego. Niestety, nie można ufać, że wszyscy programiści będą wykorzystywać kompilatory dostarczane przez oficjalnych producentów i nie będą dokonywać bezpośrednich zmian w uzyskanym kodzie pośrednim *byte-code*. Co za tym idzie, największa odpowiedzialność za zabezpieczenie komputera użytkownika spoczywa na wirtualnej maszynie Java, której zadanie sprowadza się do kompleksowej izolacji sprowadzanych z sieci publicznej apletów.

Załadowanie kodu wykonywalnego programu jest wykonywane przez ClassLoader, będący jednym z kluczowych elementów JVM. Po załadowaniu apletu, ClassLoader tworzy dla niego oddzielną "przestrzeń nazw", celem zapewnienia unikalności i możliwości rozróżniania obiektów, metod i atrybutów różnych aplikacji, posiadających pokrywające się nazwy. W razie potrzeby ClassLoader uaktywnia moduł kontrolny Verifier, który dokonuje szczegółowej analizy kodu *byte-code* w zakresie:

- sprawdzenia zgodności ze specyfikacją języka;
- wykrycia nieprawidłowości zarządzania pamięcią;

- kontroli integralności systemu "przestrzeni nazw";
- wykrycia prób nielegalnej konwersji typów danych;
- sprawdzenia czy aplet próbuje ingerować w mechanizm zabezpieczeń VJM.

Ostatnim ogniwem łańcucha zabezpieczeń jest komponent Security Manager, odpowiedzialny za kontrolę zachowania apletów w trakcie działania. Security Manager nie zezwala aby aplety sprowadzone z sieci dokonywały:

- zapisu i odczytu plików;
- usuwania plików;
- uzyskiwania informacji na temat plików;
- uruchamiania innych programów;
- wywoływania komend systemu operacyjnego;
- modyfikowania wątków systemowych;
- wykorzystywania lokalnych bibliotek;
- wywoływania metod języka C++;
- otwierania niedozwolonych połączeń sieciowych - aplet może prowadzić komunikację sieciową wyłącznie z komputerem, z którego został sprowadzony.

Większość producentów oprogramowania stara się, aby szczegóły zastosowanych w ich produktach zabezpieczeń utrzymywać w ścisłej tajemnicy.

SUN Microsystems zastosował zupełnie odmienną strategię działania - pełna specyfikacja wraz z kodem źródłowym języka Java jest dostępna publicznie. Nie ulega wątpliwości, iż każde współczesne oprogramowanie posiada błędy, a Java nie jest pod tym względem żadnym wyjątkiem. Ujawnienie szczegółów implementacyjnych ma na celu wykrycie jak największej ilości błędów. Obecnie wiele niezależnych organizacji podejmuje się zadania sprawdzania poprawności tej technologii. Szczególnym zainteresowaniem cieszy się oczywiście wyszukiwanie "dziur" w systemie zabezpieczeń. Na uwagę zasługuje działalność uniwersytetów Princeton i Oxford, które doprowadziły do wykrycia wielu poważnych niedociągnięć pierwszych implementacji Java.

Stosowanie restrykcyjnej polityki bezpieczeństwa jest dobre jedynie w odniesieniu do pewnych prostych aplikacji, których zadanie ogranicza się do urozmaicania dokumentów hipertekstowych WWW. Warunkiem poprawnego funkcjonowania dużej części oprogramowania użytkowego (np. edytory tekstu, arkusze kalkulacyjne) jest możliwość bezpośredniego korzystania z systemu plików komputera. Dla takich programów model bezpieczeństwa zastosowany w obecnej implementacji Java nie jest odpowiedni. Najnowsza wersja Java Developer Kit (JDK) zawiera propozycję rozwiązania tego problemu.

JDK 1.1 umożliwia wykonywanie podpisów cyfrowych, pozwalających na jednoznaczne określenie miejsca pochodzenia aplikacji oraz sprawdzenie czy kod programu nie został zmodyfikowany. Dzięki temu będzie można zezwolić, aby programy pochodzące z "zaufanych" serwerów aplikacji były traktowane podobnie jak programy lokalne. Oprócz podpisów cyfrowych JDK 1.1 przewiduje możliwość prowadzenia szyfrowanej komunikacji sieciowej pomiędzy odległymi procesami klienta i serwera, funkcjonującymi w ramach aplikacji rozproszonej. JDK 1.1 obejmuje pakiet *java.security,* zawierający między innymi realizację algorytmów DSA, MD5 oraz SHA. *Java.security* zawiera interfejsy, które mogą być zaimplementowane przez innych producentów. *JavaSoft* dostarcza program Java ARchive (JAR), który umożliwia grupowanie wielu plików należących do jednej aplikacji (np. pliki wykonywalne, graficzne, muzyczne), tak aby mogły być później oznaczone jednym podpisem

cyfrowym. JDK 1.1 zawiera program javakey, który pozwala na generowanie i zarządzanie kluczami i certyfikatami oraz wykonywanie podpisów cyfrowych plików JAR. Ostatnim, choć nie najłatwiejszym w użyciu mechanizmem bezpieczeństwa technologii Java jest analizator kodu pośredniego *byte-code.* Aplikacja ta udostępniana oficjalnie przez *SunSoft* (np. w nowej wersji systemu Solaris 2.6) umożliwia wygenerowanie źródeł programu z jego postaci półskompilowanej.

Dla środowiska Intranetu funkcjonującego tylko w oparciu o lokalne serwery aplikacji zagadnienie bezpieczeństwa języka Java posiada marginalne znaczenie. Jest mało prawdopodobne, aby lokalny serwer udostępniał programy, które będą atakować stacje robocze użytkowników. Współczesne technologie "firewall" (np. Solstice FireWall-1 od 3.0) pozwalają na prowadzenie selekcji napływających do sieci lokalnej apletów, dzięki czemu można zezwolić na korzystanie z usług tylko określonych serwerów zewnętrznych, np. serwerów oddalonego oddziału organizacji. Dodatkowo można prowadzić "odfiltrowywanie" ActiveX, JavaScript i innych elementów "wbudowywanych" w strony HTML, które mogą zagrozić bezpieczeństwu lokalnych stacji roboczych.

7.4 Firewall

Ściana ogniowa (gateway ochronny) chroni sieć przed intruzami z zewnątrz. Opierając się na badaniach laboratoryjnych przeprowadzonych przez *National Software Testing Laboratories* i *Data Communications* (wyniki testów są ogólnie dostępne w sieci Internet pod adresem: http://www.data.com/Lab_Tests/Firewalls.html), można wyłonić pewne wyróżniające się rozwiązania:

- Borderware Firewall Server - *Border Network Technologies*;
- Firewall-1 - *Checkpoint Software Technologies* lub popularna wersja OEM z *SunSoft;*
- Digital Firewall for Unix - *DEC*;
- Cyberguard - *Harris Computer Systems Corporation*.

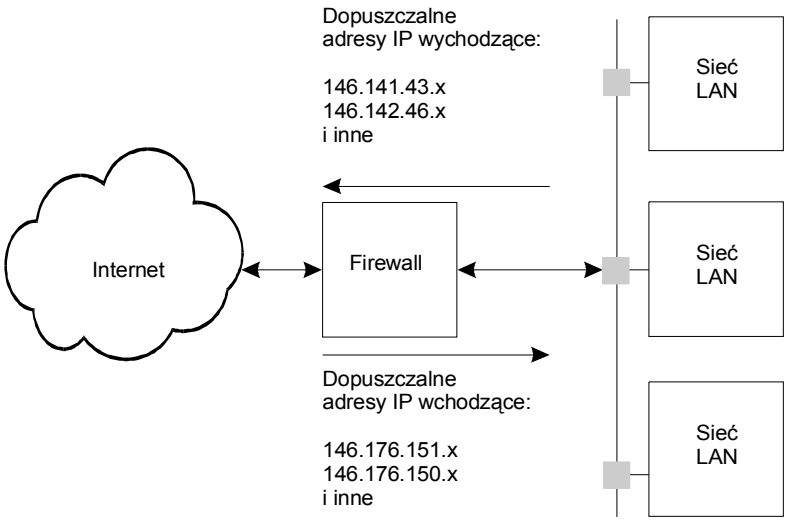
Najwyższe wyniki testów, spośród wyżej wymienionych produktów, uzyskał Firewall-1. Firewalle różnią się między sobą sposobami podejścia do zagadnienia bezpieczeństwa i mogą być podzielone na:

- blokujące ruch;
- nadzorujące i zezwalające na ruch.

Filtry pakietów

Filtr pakietów jest najprostszą formą firewalla. W swym algorytmie pracy utrzymują informacje na temat uprawnionych adresów źródeł i ujść i kasują wszystkie pakiety zawierające inne adresy. Technika ta jest nazywana filtracją pakietów. Filtr pakietów utrzymuje tablice źródeł i ujść informacji dla obu kierunków współpracy, to znaczy do i z Internetu. Taka metoda ochrony jest pożyteczna dla firm o geograficznie rozproszonych filiach. Tak, więc filtr pakietów zezwala na ruch przychodzący z innych „przyjaznych" miejsc i blokuje ruch „nieprzyjazny". Przedstawiono to na rysunku 7.5.

Niestety metoda ta, w przypadku fałszowania adresów IP, jest zawodna. Dla przykładu, „hacker" może określić listę adresów mających certyfikat „przyjazności" a następnie generować pakiety o określonym adresie IP, które są adresowane do sieci Intranetowej.

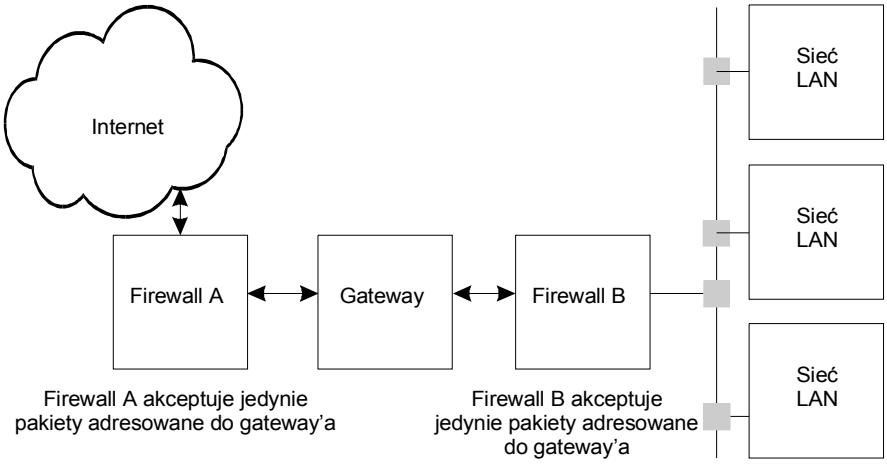


Rysunek 7.5 Filtr pakietów

Gateway poziomu aplikacji

Gatewaye poziomu aplikacji posiadają dodatkową warstwę ochrony zwiększającą bezpieczeństwo połączeń pomiędzy Intranetem i Internetem. Gatewaye posiadają trzy główne komponenty:

- węzeł gatewaya;
- dwie ściany ogniowe po obydwu stronach gatewaya, przesyłające pakiety przeznaczone do albo od gatewaya.



Rysunek 7.6 Gateway poziomu aplikacji

Rysunek 7.6 przedstawia gateway z warstwą aplikacyjną. Firewall A odrzuca wszystko, co nie jest adresowane do węzła gatewaya a także wszystko, co nie jest wysyłane przez węzeł gatewaya. Zatem transfer plików z sieci lokalnej do użytkownika sieci globalnej musi odbywać się następująco:

- zalogowanie się na węźle gatewaya;
- transfer pliku do gatewaya;
- transfer pliku z gatewaya do sieci globalnej.

W celu skopiowania pliku do sieci wewnętrznej, zewnętrzny użytkownik musi:

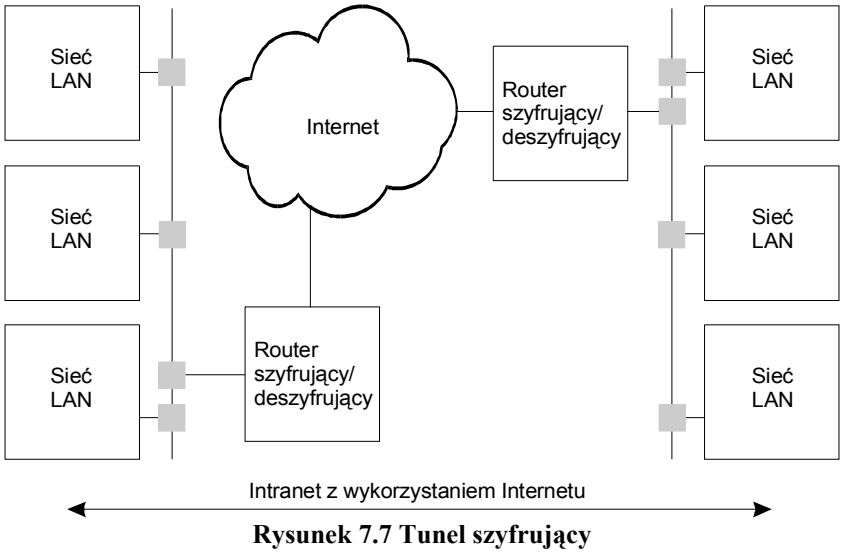
- zalogować się na węźle gatewaya;

– przesłać plik z sieci globalnej do gatewaya.

Następnie gateway transferuje plik do sieci lokalnej. Ogólna strategia organizacji współpracy pozwala na swobodny przepływ poczty elektronicznej pomiędzy Internetem i siecią lokalną, zaś transfer plików i operacja zdalnego logowania odbywają się w specjalny sposób. Niestety, poczta elektroniczna może także być wykorzystywana do transferu plików. Aby rozwiązać ten problem, firewall może nadzorować także przepływ poczty elektronicznej a w szczególności wiadomości pocztowej o dużej objętości, prowadząc limitowanie możliwego rozmiaru transferowanych plików. Taka metoda nie jest niestety wygodna, bo wymusza podział dużych plików na małe części i oddzielne ich przesyłanie.

Tunele szyfrujące

Filtry pakietów i gatewaye warstwy aplikacyjnej eliminują w dużym stopniu niebezpieczeństwo dostępu do sieci lokalnej nieprzyjaznych gości. Jednakże filtr pakietów może być oszukiwany, jeśli zostaną podmienione adresy IP (IP spoofing), zaś do gatewaya z poziomem aplikacyjnym można włamać się w przypadku określenia haseł użytkowników gatewaya a następnie prowadzić transmisję plików z sieci do firewalla. Następnie do gatewaya a potem, z firewalla na zewnątrz. Najlepszą metodą zabezpieczenia przed tego typu atakami jest ograniczenie liczby użytkowników uprawnionych do transferu plików przez gateway.



Rysunek 7.7 Tunel szyfrujący

Najlepszą metodą ochrony jest szyfrowanie wiadomości opuszczających sieć i deszyfrowanie wiadomości wchodzących z zewnątrz (rysunek 7.7). Klucze wymagane w procesie szyfrowania i deszyfrowania znane są jedynie przyjaznym użytkownikom. Metoda ta ma taką dodatkową zaletę, że dane nie są łatwe do podsłuchania.

Za szyfrowanie i deszyfrowanie odpowiadają routery, które są bezpośrednio przyłączone do sieci Internet.

Aplikacja firewall

Firewall-1 jako jedno z nielicznych rozwiązań prowadzi bieżące monitorowanie stanu wszystkich otwartych sesji komunikacji sieciowej, niezależnie od tego czy transmisja danych prowadzona jest w oparciu o komunikację połączeniową (TCP) czy bezpołączeniową (UDP). Dużą zaletą tego oprogramowania jest także przejrzysty

interfejs graficzny użytkownika, który w znacznym stopniu usprawnia proces wdrażania i nadzorowania realizacji przyjętej strategii ochrony. Dzięki zastosowaniu algorytmów selektywnej filtracji pakietów, Firewall-1 bardzo nieznacznie obniża efektywność funkcjonowania całego systemu.
Zestaw potencjalnych możliwości Firewall-1 obejmuje:
- filtrację pakietów (przeciwdziałanie "spoofing");
- aplikacje pośredniczące (*ang. application proxy*) (prowadzenie identyfikacji, kontroli tożsamości, kontroli uprawnień);
- translację adresów internetowych (ukrywanie wewnętrznych adresów IP);
- szyfrowanie i uwierzytelnianie, tworzenie wirtualnych sieci prywatnych (*ang. virtual private network*).

7.5 Wybrane zagadnienia z kryptografii w sieci Internet

Jednym z najistotniejszych zagadnień związanych z wykorzystaniem tej technologii jest bezpieczeństwo. Jak wykazują badania statystyczne, ponad 70% odnotowanych przypadków "włamań" do systemów informatycznych zostało przeprowadzone przez użytkowników lokalnych.

Jednym z najbardziej skutecznych sposobów utrzymywania prywatności posiadanych i przekazywanych informacji jest szyfrowanie. Proces szyfrowania danych polega na przekształceniu ich do postaci niejawnego szyfrogramu tak, aby dane mogły być odczytane wyłącznie przez osoby do tego upoważnione. Szyfrowanie odbywa się zgodnie z pewnym przyjętym algorytmem matematycznym, a uzyskana wartość szyfrogramu zależy od zastosowanego klucza.

Szyfrowanie wiadomości kluczem tajnym

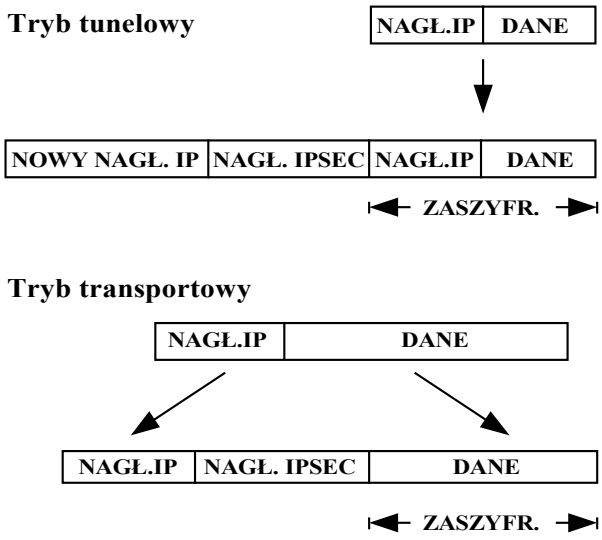
Tradycyjne algorytmy kryptograficzne, określane mianem systemów szyfrowych z kluczem tajnym, zakładają użycie identycznego klucza do szyfrowania i deszyfrowania. Jest oczywiste, iż wartość tego klucza musi być utrzymywana w ścisłej tajemnicy. Wartość algorytmu szyfrującego zależy od jego odporności na kryptoanalizę, a w szczególności "atak brutalny". "Atak brutalny" (ang. *force attack*) ma na celu wyznaczenie formy jawnej informacji na podstawie kryptogramu, bez znajomości klucza szyfrowania i polega na sprawdzaniu całej przestrzeni klucza, a jego powodzenie zależy w głównej mierze od długości klucza przyjętego dla określonego algorytmu szyfrowania. Kryptoanaliza jest działem kryptologii, która zajmuje się analizą algorytmów kryptograficznych pod kątem wyszukiwania ich słabych punktów.

DES

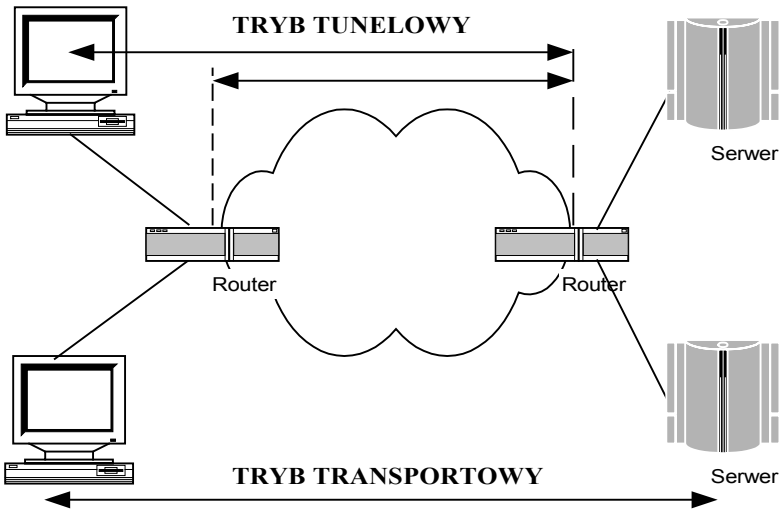
Pierwszym, rozpowszechnionym na szeroką skalę systemem szyfrowym klucza tajnego jest DES (*ang. Data Encryption Standard*), opracowany w latach 70-tych przez IBM (projekt Lucifer). DES od ponad 15 lat jest światowym standardem szyfrowania i mimo tak pokaźnego wieku nie poddał się licznym próbom kryptoanalizy (rysunek 7.8 i 7.9 aplikacja DES- IPSec). Ostatnio, z uwagi na dynamiczny rozwój mikroelektroniki komputerowej, dużo wątpliwości wzbudza podatność algorytmu na próbę "ataku brutalnego". Przy długości klucza wynoszącej 56 bitów jest 2^{56} możliwych kluczy, czyli w przybliżeniu $7.2*10^{16}$ kluczy. Atak metodą brutalną (kolejnego podstawiania klucza) przy nakładach 1 000 000 $ trwałby 3.5 godziny przy nakładzie 100 000 $ 35 godzin (za Williamem Stalingsem „Ochrona danych w sieci i intersieci” Prentice Hall 1994r),

ponieważ zastosowany w DES klucz o długości 56 bitów daje potencjalną możliwość pomyślnego przeprowadzenia takiej próby.

DES jest także znany pod nazwą DEA (*ang. Data Encryption Algorithm*) nadaną mu przez Amerykański Narodowy Instytut Standaryzacji ANSI. Istnieje wiele zmodyfikowanych implementacji DES, których powstanie miało na celu zwiększenie szybkości szyfrowania i wzmocnienie tradycyjnego algorytmu np. "Potrójny DES" (ang. Triple DES), "Uogólniony DES" (*ang. Generalized DES*), CRYPT(3) i inne.



Rysunek 7.8 Tryby pracy IPSec



Rysunek 7.9 Sposoby wykorzystania trybów pracy IPSec

RSA

Wśród innych, komercyjnie wykorzystywanych systemów szyfrowych klucza tajnego najbardziej rozpowszechnione są algorytmy RC2 i RC4, zaprojektowane przez Rona Rivesta dla *RSA Data Security*. RC2 i RC4 to algorytmy kryptograficzne o zmiennej długości klucza szyfrowania. Szczegóły projektu obu algorytmów nigdy nie

zostały oficjalnie opublikowane i trudno jest coś powiedzieć na temat ich odporności na kryptoanalizę. Wydaje się, więc, iż poziom bezpieczeństwa informacji dawany przez RC2 i RC4 zależy w głównej mierze od długości zastosowanego klucza szyfrowania, a ten z kolei jest ograniczony (do 40 bitów) przez restrykcyjne prawo eksportowe USA. Panuje opinia, iż USA nie pozwala na eksport algorytmu, którego nie potrafiłaby (przynajmniej teoretycznie) złamać.

IDEA

W ostatnim czasie dużą popularność zyskuje algorytm IDEA (*ang. International Data Encryption Algorithm*), opracowany na początku lat 90-tych przez Xuejia Lai i Jamesa Masseya. Bruce Schneier, autor popularnej książki "Kryptografia dla praktyków." (oryginał: "Applied Cryptography") uważa, że IDEA to obecnie najlepszy i najbardziej bezpieczny w swojej klasie, dostępny publicznie algorytm szyfrowania. Dzięki zastosowaniu klucza szyfrowania o długości 128 bitów, IDEA wydaje się być algorytmem odpornym na "atak brutalny" - należałoby bowiem wykonać 2^{128} prób szyfrowania, co przy współczesnym poziomie technologii jest praktycznie niewykonalne. Jeżeli chodzi o inne próby kryptoanalizy, to z uwagi na krótki czas istnienia tego algorytmu, nie można na ten temat dużo powiedzieć. Oprócz przedstawionych algorytmów istnieje jeszcze wiele innych, mniej znanych implementacji np. REDOC-II, REDOC-III, Khufu, CA-1.1 i inne.

Szyfrowanie wiadomości kluczem jawnym

W odniesieniu do środowiska sieci komputerowych stosowanie systemów szyfrowych klucza tajnego jest bez wątpienia bardzo uciążliwe z uwagi na konieczność ciągłego utajniania kluczy szyfrowania. Jak do tej pory nie wynaleziono środka transportu poprzez który można by było sprawnie przekazywać tajny klucz pomiędzy nadawcą i odbiorcą informacji, szczególnie przy prowadzeniu częstych sesji komunikacyjnych gdy czas przekazywania danych nie jest obojętny.

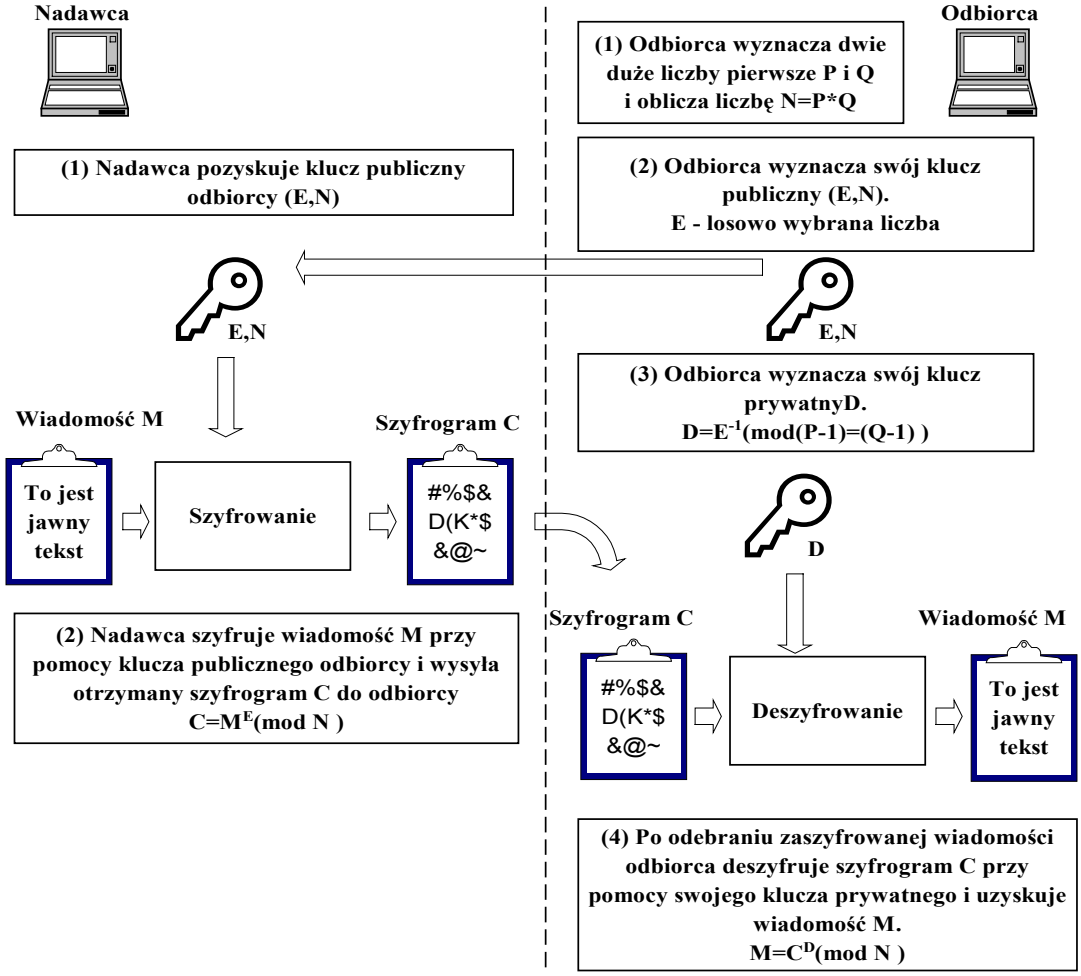
Propozycją rozwiązania tego problemu są systemy szyfrowe z kluczem jawnym (publicznym), które pozwalają na prowadzenie szyfrowania danych bez konieczności wcześniejszej wymiany tajnych informacji. Systemy szyfrowe klucza jawnego zakładają, iż każda ze stron uczestniczących w procesie szyfrowania/deszyfrowania informacji jest wyposażona w parę matematycznie zależnych kluczy: klucz prywatny (tajny) i klucz publiczny (jawny). Dane zaszyfrowane jednym z tych kluczy mogą być rozszyfrowane wyłącznie przy użyciu odpowiadającego mu drugiego klucza. Przyjęte jest, iż klucz prywatny podlega ścisłej ochronie i nigdy nie opuszcza maszyny swojego właściciela w odróżnieniu od klucza publicznego, który może być rozprowadzany publicznie bez żadnych ograniczeń.

RSA

Algorytm RSA opracowany został przez Rona Rivesta, Adi Shamira i Leonarda Adelmana. RSA został wprowadzony w 1978 roku i aż do dziś nie poddał się licznym próbom kryptoanalizy.

Rysunek 7.10 przedstawia uproszczoną zasadę działania tego algorytmu. Nadawca informacji dokonuje ich zaszyfrowania przy pomocy klucza publicznego odbiorcy. Tak zaszyfrowane informacje mogą zostać odszyfrowane wyłącznie przez odbiorcę, ponieważ tylko on posiada odpowiedni klucz prywatny. RSA jest często wykorzystywany do szyfrowania danych przesyłanych w sieciach komputerowych, a jego popularność wynika w dużej mierze ze znaczących zastosowań w Internecie. Jedną

z poważnych wad, jaką można zarzucić RSA jest szybkość działania, która w porównaniu do DES jest ok. 1000 razy mniejsza. Aby zaradzić tej sytuacji, większość popularnych systemów ochrony danych używa RSA wyłącznie do szyfrowania klucza sesji, wykorzystywanego do szyfrowania właściwych informacji przy pomocy algorytmu z kluczem tajnym (np. system ochrony poczty elektronicznej Pretty Good Privacy).

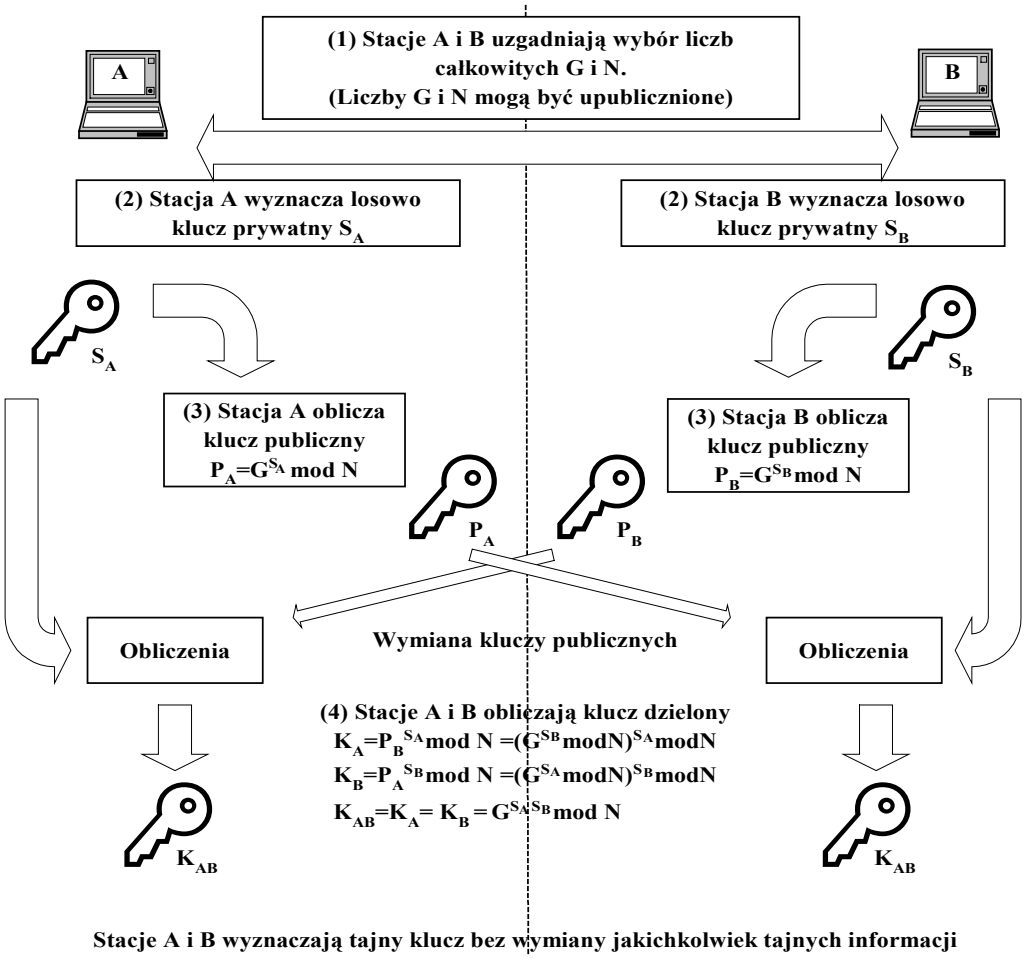


Rysunek 7.10 Koncepcja szyfrowania danych w algorytmie RSA

Algorytm Diffiego-Hellmana

Bardzo ciekawym rozwiązaniem należącym do grupy systemów szyfrowych klucza jawnego jest algorytm Diffiego-Hellmana (rysunek 7.11), którego nazwa pochodzi od nazwisk jego twórców Whitfielda Diffie i Martina Hellmana. Zasadniczo, algorytm Diffiego-Hellmana nie może być bezpośrednio wykorzystany do szyfrowania danych - algorytm pozwala, aby nadawca i odbiorca informacji mogli wyznaczyć jeden, tajny klucz szyfrowania bez konieczności wcześniejszej wymiany jakichkolwiek poufnych informacji.

Tak wyznaczony klucz może być później wykorzystany do szyfrowania danych przy pomocy któregoś z systemów szyfrowych klucza tajnego (np. DES, IDEA, RC4). Rysunek przedstawia koncepcję tego algorytmu. Obok RSA, algorytm Diffiego-Hellmana jest najpopularniejszym systemem szyfrowym z kluczem jawnych wykorzystywanym w sieci Internet.



Stacje A i B wyznaczają tajny klucz bez wymiany jakichkolwiek tajnych informacji

Rysunek 7.11 Zasada działania algorytmu Diffiego-Hellmana

7.6 Integralność informacji

Niekiedy, szczególnie w przypadku przesyłania poufnych dokumentów za pośrednictwem sieci komputerowej, ważną rolę odgrywa kwestia potwierdzania integralności otrzymywanych informacji - odbiorca chciałby być pewny, że dane nie zostały zmodyfikowane w czasie transmisji. Zapewnienie integralności przesyłanych informacji uzyskuje się najczęściej poprzez utworzenie tzw. skrótu komunikatu (*ang. message digest*) przy pomocy odpowiedniego algorytmu matematycznego.

Algorytmy takie określane są mianem jednokierunkowych funkcji skrótu z uwagi na swoje właściwości. Obliczenie skrótu wiadomości sprowadza się do podania tej wiadomości jako argumentu jednokierunkowej funkcji skrótu. Termin *jednokierunkowa* oznacza, że nie powinno być możliwości wyznaczenia treści wiadomości na podstawie jej skrótu.

Jednokierunkowe funkcje skrótu określane są także jako funkcje haszujące z uwagi na dodatkowe wymaganie, które zakłada, iż znalezienie dwóch różnych wiadomości mających takie same skróty powinno być bardzo trudnym zadaniem. Wśród najbardziej rozpowszechnionych funkcji można wyróżnić MD2 i MD5 opracowane przez Rona Rivera oraz tzw. bezpieczny algorytm haszujący SHA (ang. *Secure Hash Algorithm*) zaproponowany przez amerykański *Narodowy Instytut Standardów i Technologii NIST* wraz z *Narodową Agencją Bezpieczeństwa NSA*.

7.7 Autentyczność informacji

Analiza skrótu wiadomości pozwala wykryć czy wiadomość w czasie transmisji została zmodyfikowana, jednak nie gwarantuje jej autentyczności, tzn. nie można jednoznacznie określić, przez kogo została wysłana. Najczęściej stosowaną techniką uwierzytelniania informacji jest tworzenie tzw. podpisów cyfrowych (*ang. digital signature*). Podpis cyfrowy może zostać wykonany poprzez zaszyfrowanie skrótu wiadomości przy użyciu klucza prywatnego nadawcy. Jeżeli odbiorca będzie w stanie odszyfrować podpis cyfrowy przy pomocy klucza publicznego nadawcy to może być pewny, że podpis cyfrowy został wykonany przez nadawcę i tym samym potwierdzić autentyczność otrzymanych informacji. Wykonanie podpisu cyfrowego może być zrealizowana przy pomocy omawianego już systemu RSA. W ostatnim czasie dużą popularność zyskuje algorytm DSA (*ang. Digital Signature Algorithm*) zaproponowany przez *NIST* jako standard tworzenia podpisów cyfrowych (znany także pod nazwą DSS *ang. Digital Signature Standard*).

8 Sieci dostępowe dla usług teleinformatycznych

8.1 Ogólny model odniesienia dla sieci dostępowych

Architektura sieci dostępowych

Użycie światłowodów w sieciach dostępowych i stopniowe eliminowanie kabli miedzianych staje się coraz powszechniejsze. Odzwierciedleniem tego zjawiska są systemy FITL (*ang. Fibre In The Loop*). Wychodzą one naprzeciw stale rosnącym wymaganiom stawianym operatorom publicznych sieci telekomunikacyjnych. Oprócz zapewnienia podstawowych usług telekomunikacyjnych, takich jak łączność telefoniczna, coraz więcej mówi się o możliwości świadczenia usług wykraczających poza podstawowy zakres. Mowa tu między innymi o usługach multimedialnych, takich jak wideo na żądanie (*ang. Video on Demand*), tele i wideo konferencje, wideotelefon, szybki dostęp do sieci Internet, wirtualne sieci LAN, transmisja cyfrowa dźwięku o jakości CD, elektroniczne zakupy i inne. Aby możliwe było dostarczenie tego typu usług, powstało kilka koncepcji przebudowy lub też budowy dostępowych sieci abonenckich (*ang. Access Networks*), których zadaniem byłoby dostarczenie wyżej wymienionych usług do abonentów publicznych sieci telekomunikacyjnych. Jedną z technik wykonania takich sieci dostępowych są właśnie systemy FITL. Sieci FITL wykorzystują technikę światłowodową, która zakłada stosowanie nośników optycznych w magistralnej oraz rozdzielczej części sieci telekomunikacyjnej. Zależnie od ulokowania optycznej jednostki sieciowej ONU (*ang. Optcal Network Unit*) można wyróżnić trzy architektury sieci:

- światłowód doprowadzony do mieszkania FTTH (*ang. Fibre To The Home*),
- światłowód doprowadzony do budynku FTTB (*ang. Fibre To The Bulding*),
- światłowód doprowadzony do szafki przy ulicy FTTC (*ang. Fibre To The Curb*).

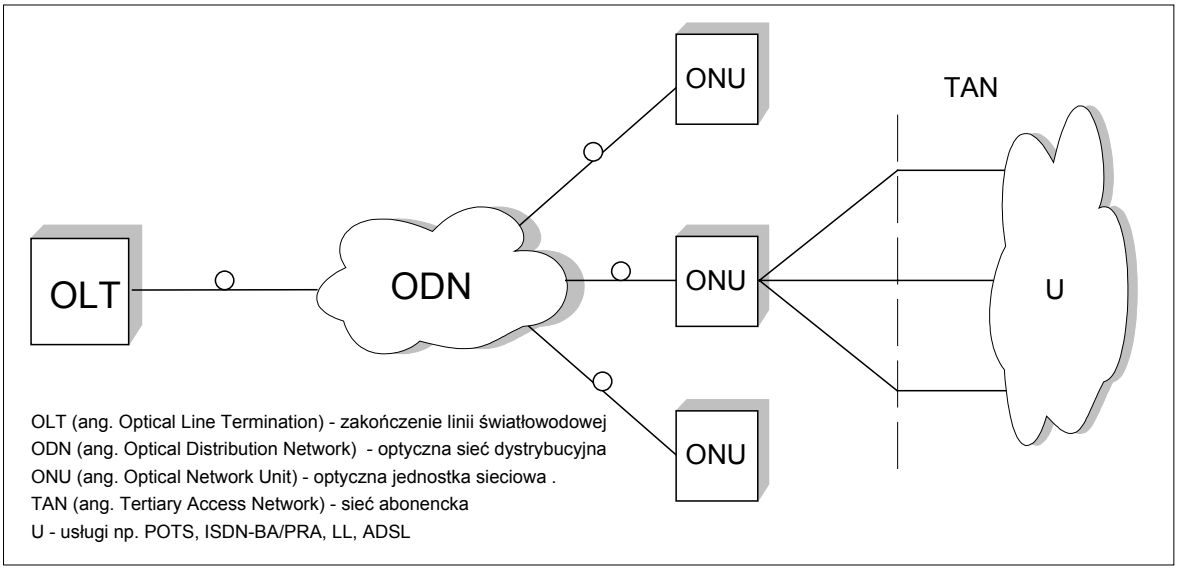
Nazwa architektury opisuje miejsce instalacji ONU. Wszystkie te rozwiązania przewidują wykorzystanie kabla światłowodowego w części magistralnej sieci. Najbardziej zaawansowane rozwiązanie –FTTH, to sieć abonencka używająca całkowicie światłowódu, aż do użytkownika. Jest to rozwiązanie najdroższe i jak dotąd najrzadziej stosowane.

Systemy FITL współpracują z istniejącą siecią telekomunikacyjną. Muszą być więc zdolne do współpracy z centralami telefonicznymi wyposażonymi w zarówno cyfrowe, jak i analogowe pola komutacyjne. Inną ważną cechą systemów FITL jest możliwość realizacji zarówno tradycyjnych wąskopasmowych usług telekomunikacyjnych, jak też nowych usług szerokopasmowych.

Na rysunku 8.1 przedstawiono ogólny schemat blokowy architektury systemu FITL. Składa się on z następujących elementów:
zakończenie linii światłowodowej OLT (*ang. Optical Line Termination*), nazywane przez niektórych producentów cyfrowym terminalem centralowym HDT (*ang. Host Digital Termination*),
optyczna sieć dystrybucyjna ODN (*ang. Optical Distribution Network*),
optyczne jednostki sieciowe ONU (*ang. Optical Network Unit*).

Zakończenie linii optycznej OLT stanowi rodzaj styku sieci dostępowej z punktem dostępu do usług telekomunikacyjnych. Fizyczne połączenie pomiędzy OLT oraz jedną, bądź większą liczbą wyniesionych jednostek optycznych ONU, jest zrealizowane za pośrednictwem sieci dystrybucyjnej ODN na jednym lub dwóch włóknach światłowodowych, w zależności od zastosowanego sposobu transmisji (simpleks lub

dupleks). ONU transmituje między ODN a abonentem sygnały odpowiadające informacji. Urządzenie końcowe przetwarza odebrany sygnał na informację. Punktem styku użytkownika z siecią dostępową jest gniazdko abonenckie.



Rysunek 8.1 Architektura sieci dostępowych FITL

Zastosowanie światłowodu w pętli abonenckiej FITL obejmuje trzy wcześniej wymienione konfiguracje:

- FTTC *ang. Fibre To The Curb*,
- FTTB *ang. Fibre To The Building*,
- FTTH *ang. Fibre To The Home*,
- HFC *ang. Hybrid Fiber Coax*.

Rozwiązania te zapewniają wystarczające pasmo transmisyjne dla obecnych i przyszłych aplikacji interaktywnych i dystrybucyjnych zarówno wąskopasmowych jak i szerokopasmowych.

FTTC - jest rozwiązaniem efektywnym pod względem ceny dla osiedli mieszkaniowych, gdzie znajduje się wiele domów. W tym przypadku światłowód dochodzi do odpornej na zmienne warunki atmosferyczne szafki usytuowanej w pobliżu drogi, stanowiącej zakończenie toru światłowodowego. Podłączenie do użytkowników zapewniają tzw. odcinki końcowe (*ang. last drop*), w miarę możliwości wykorzystujące istniejącą już skrętkę lub pary miedziane. Zaletą tego podejścia jest to, że koszt takiego rozwiązania jest dzielony pomiędzy wielu abonentów. W konsekwencji taryfy mogą być utrzymywane na niskim poziomie, co prowadzi do szybszego rozpowszechniania się usług.

FTTB - jest architekturą dedykowaną dla abonentów w dużych budynkach umożliwiającą dostarczanie zaawansowanych usług multimedialnych. Podobieństwo do FTTC polega na tym, iż koszt rozkłada się na wielu użytkowników. Różnica polega na tym, że sieć dystrybucyjna kończy się w budynku, zwykle w piwnicy lub w studzience telekomunikacyjnej. Podobnie jak w poprzednim rozwiązaniu, końcowe podłączenie do użytkowników jest wykonane poprzez skrętkę lub pary miedziane.

FTTH- polega na doprowadzeniu osobnego światłowodu do mieszkania (domu) każdego abonenta systemu. Jest to najbardziej optymalne rozwiązanie dostępu

sieciowego. Zapewnia ono pełną szerokość pasma, jaką posiada łącze światłowodowe dla każdego użytkownika. W konsekwencji zakres usług, jaki można dostarczyć abonentowi jest w zasadzie nieograniczony.

HFC - jest to rozwiązanie, w którym łączy się w obszarze sieci dostępu sygnały przesyłane kablami współosiowymi i światłowodami. W sieci abonenckiej wykorzystywany jest przewód współosiowy do transmisji sygnałów telefonicznych i telewizyjnych. Sygnały telewizyjne z głównej stacji czołowej systemu przesyłane są do stacji lokalnych (*ang. Hub Head End*), z których rozsyłane są światłowodami do szerokopasmowych optycznych zakończeń sieciowych (B)ONT. Do zakończeń tych doprowadzane są także światłowodem sygnały w grupach n×2Mbit/s z węzłów dostępu.

8.2 Elementy funkcjonalne w architekturze sieci FITL

Zakończenie linii światłowodowej OLT

Zakończenie linii światłowodowej OLT zarządza przyłączonymi wyniesionymi jednostkami optycznymi ONU oraz zapewnia połączenie systemu FITL z pozostałą częścią publicznej sieci telekomunikacyjnej. OLT może być umieszczone zarówno w budynku samej centrali telefonicznej jak też w innym odpowiednio przygotowanym pomieszczeniu. Węzeł OLT jest wyposażony w interfejsy służące połączeniu sieci dostępowej z siecią publiczną oraz moduły niezbędne do komunikacji z ONU. OLT może zarządzać systemem sygnalizacji oraz nadzoru poszczególnych optycznych jednostek sieciowych ONU, m.in. odpowiada za kontrolę zabezpieczeń i utrzymanie działania. Do funkcji zarządzania sygnalizacją można między innymi zaliczyć zmiany formatu przesyłanych wiadomości sygnalizacyjnych (np. interfejsy V5.1 i V5.2).

Optyczna sieć dystrybucyjna ODN

Optyczna sieć dystrybucyjna ODN ma za zadanie fizyczne połączeniu OLT z optycznymi jednostkami sieciowymi ONU. Można wyróżnić dwa rodzaje sieci: pasywną oraz aktywną.

Sieci pasywne PON (*ang. Passive Optical Network*) są zbudowane z pasywnych elementów optycznych. Medium transportowym jest światłowód jednomodowy. Sygnał optyczny przenoszony przez włókno światłowodowe jest rozdzielany na kilka wiązek w pasywnych rozgałęźnikach optycznych (*ang. Splitter*). Współczynnik podziału rozdzielaczy przyjmuje wartości od 1:2 do 1:65, zależnie od oczekiwanego zasięgu danego odcinka światłowodu. Pasywne rozdzielacze sygnału nie wymagają zasilania. Upraszcza to budowę sieci dystrybucyjnej oraz redukuje koszty wykonania i utrzymania sieci dostępowej. Optyczna sieć dystrybucyjna może być wykonana zarówno w konfiguracji punkt - punkt (gdzie łącze światłowodowe jest prowadzone od zakończenia linii światłowodowej OLT do ONU), jak też w konfiguracji punkt - wielopunkt (gdzie element rozgałęziający sygnał jest umieszczony wewnątrz ODN i łączy OLT z wieloma ONU).

Sieci aktywne AON (*ang. Active Optical Network*) mogą wykorzystywać technologie PDH lub SDH w postaci ringu światłowodowego, w którym OLT stanowi jeden z elementów włączonych do ringu służący do zapewnienia połączenia z siecią publiczną a optyczne jednostki sieciowe ONU wyposażone w odbiorniki/nadajniki regenerują sygnał w światłowodzie jednocześnie zapewniając połączenie poprzez łącza końcowe z abonentami systemu.

Optyczne jednostki sieciowe ONU

Optyczna jednostka sieciowa ONU odbiera optyczny sygnał z sieci ODN. Sygnały po stronie abonenckiej transmitowane są do interfejsu sieciowego każdego z abonentów za pomocą klasycznej sieci dostępowej, najczęściej wykonanej na bazie symetrycznej pary, skrętki lub kabla koncentrycznego. ONU posiada możliwość konwersji sygnału optycznego na elektryczny oraz odwrotnie. Spełnia również funkcje przetwornika A/C dla sygnałów o częstotliwości akustycznej.

Architektura optycznej sieci dystrybucyjnej ODN

Optyczna sieć dystrybucyjna ODN (*ang. Optical Distribution Network*) stanowi medium transmisyjne, łączące optyczne jednostki sieciowe ONU z zakończeniem linii światłowodowej OLT. Pasywna sieć dystrybucyjna PON składa się z pasywnych elementów optycznych, takich jak jednodomowe włókna światłowodowe, łączniki optyczne, optyczne urządzenia rozgałęziające, tłumiki optyczne oraz spawy łączące poszczególne światłowody.

Sieć ODN jest funkcjonalnie częścią systemu FITL. W wielu przypadkach jest ona również częścią sieci magistralnej lokalnego operatora telekomunikacyjnego. Operator sieci tworząc infrastrukturę telekomunikacyjną musi wziąć pod uwagę szereg różnych czynników. Należą do nich:

- topologiczne rozmieszczenie abonentów,
- odległość pomiędzy OLT i planowanymi jednostkami ONU,
- zdolność przenoszenia usług o różnym charakterze,
- aktualnie dostępne technologie,
- poziom mocy sygnału optycznego,
- wykorzystanie odpowiednich okien optycznych,
- możliwości dalszej rozbudowy,
- niezawodność,
- sterowanie i utrzymanie,
- zasilenie jednostek ONU,
- bezpieczeństwo sieci,
- przewidywany strumień danych od OLT do użytkowników.

Na rysunku 8.2 pokazano konfigurację sieci dystrybucyjnej ODN. Pod pojęciem sieci dystrybucyjnej ODN należy rozumieć wszystkie elementy, które znajdują się pomiędzy dwoma punktami odniesienia S i R. Punkty te są zdefiniowane następująco:

S - jest to punkt znajdujący się na wyjściu sieci ODN, w punkcie złączenia ONU i OLT, przy nadawaniu sygnału w linię,

R - jest to punkt znajdujący się na wejściu sieci ODN, w punkcie złączenia ONU i OLT, przy odbiorze sygnału z linii.

Punkty połączeń nie są częścią sieci dystrybucyjnej. W zależności od fizycznej realizacji sieci ODN punkty S i R na każdym końcu sieci ODN mogą znajdować się na tym samym bądź na różnych włóknach światłowodowych. Sieć ODN udostępnia jeden lub więcej linii światłowodowych pomiędzy OLT a jednym bądź większą liczbą ONU. Każda linia światłowodowa jest zdefiniowana pomiędzy punktami odniesienia S i R oraz dla określonej długości fali.

W sieci ODN zdefiniowane są następujące interfejsy optyczne (rysunek 8.2):

Qr: interfejs optyczny przy punkcie odniesienia R/S pomiędzy ONU a ODN,

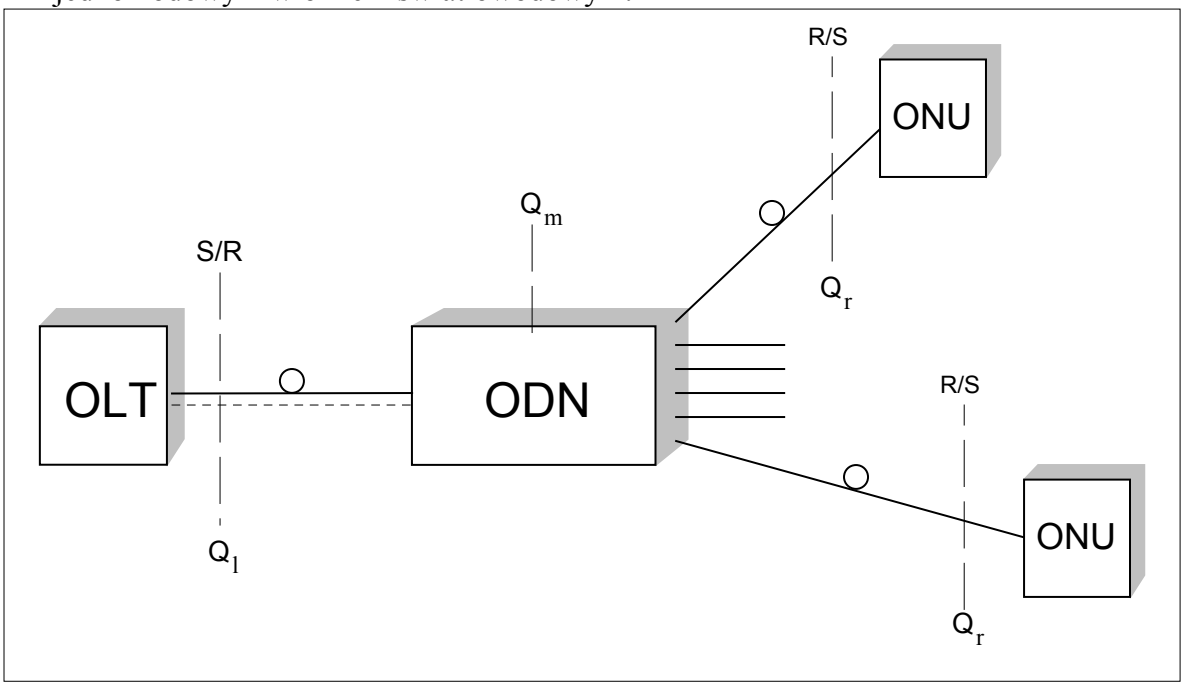
Ql: interfejs optyczny przy punkcie odniesienia S/R pomiędzy OLT a ODN,

Qm interfejs optyczny pomiędzy wyposażeniem służącym do monitorowania sieci a samą siecią ODN.

Na poziomie warstwy fizycznej interfejsy Qr i Ql mogą wymagać więcej niż jednego włókna światłowodowego dla transmisji sygnału np. w przeciwnych kierunkach bądź sygnałów dla usług różnego typu. Interfejs Qm może być umieszczony w dowolnym miejscu sieci ODN. Do swoich potrzeb może wykorzystywać zasoby sieci ODN lub korzystać z oddzielnych włókien światłowodowych.

Tak jak to było wcześniej zaznaczone, sieć dystrybucyjna ODN powinna umożliwiać realizację aktualnie dostępnych i przewidywanych w przyszłości usług bez konieczności dokonywania kosztownych modyfikacji sieci. Wymagania te w istotny sposób rzutują na parametry elementów stosowanych w sieci. Parametry mające bezpośredni wpływa na właściwości sieci to:

- przezroczystość dla różnych długości fali optycznej: urządzenia takie jak rozgałęźniki optyczne powinny mieć możliwość pracy w zakresach 1310 nm i 1550 nm,
- wzajemność: odwrócenie portów wejściowych i wyjściowych nie powinno znacząco wpływać na straty sygnału przechodzącego przez urządzenia sieci,
- zgodność optyczna: wszystkie elementy sieci powinny współpracować z jednomodowym włóknem światłowodowym.



Rysunek 8.2 Konfiguracja sieci dystrybucyjnej ODN

W sieci dystrybucyjnej ODN możliwe są dwa kierunki transmisji danych:

- do abonenta (*ang. downstream*) - transmisja od OLT w kierunku dowolnego ONU;
- od abonenta (*ang. upstream*) - transmisja od dowolnego ONU do OLT.

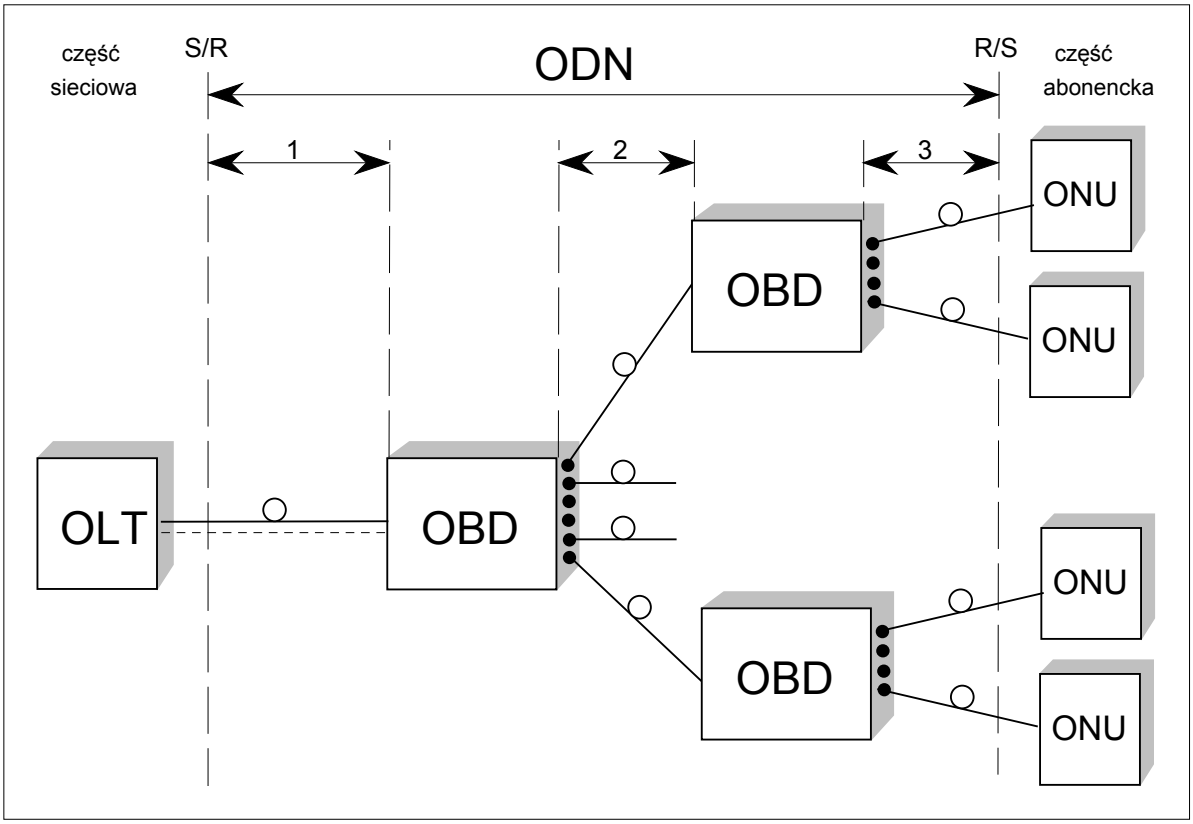
Transmisja w obu kierunkach (do i od abonenta) może być zrealizowana przy wykorzystaniu pojedynczego włókna światłowodowego w trybie simpleks lub dupleks lub przy wykorzystaniu dwóch oddzielnych włókien, po jednym dla każdego kierunku w trybie simpleks.

Charakterystyka ODN

Uwzględniając rozmaite przesłanki techniczne, ekonomiczne czy topologiczne można wyróżnić dwie podstawowe topologie sieci dystrybucyjnej: punkt - punkt oraz punkt - wielopunkt. Fizyczne połączenie jednego OLT z wieloma ONU za pośrednictwem sieci dystrybucyjnej ODN może być zrealizowane przy wykorzystaniu jednego lub dwóch światłowodów (w zależności od zastosowanego sposobu transmisji - dupleks, dipleks lub simpleks). Zastosowanie większej liczby włókien jest możliwe w celu zwiększenia niezawodności lub możliwości późniejszej rozbudowy sieci. W konfiguracji punkt - wielopunkt wyróżnia się dwie architektury:

– architektura typu drzewo,
– architektura typu magistrala.

Przykład architektury typu drzewo został przedstawiony na rysunku (rysunek 8.3).



Rysunek 8.3 Schemat architektury typu drzewo

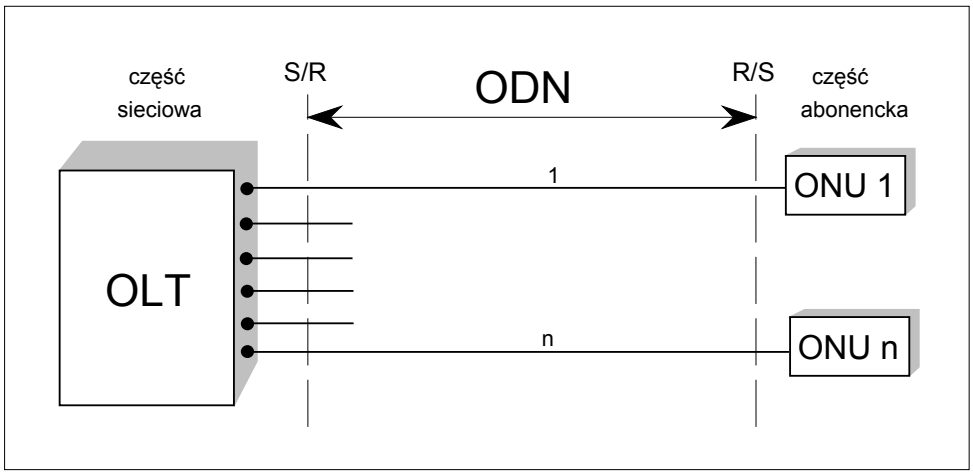
Zastosowano w niej kaskadowo połączone urządzenia rozgałęziające sygnał optyczny - OBD (*ang. Optical Branching Devices*) od OLT do ONU oraz łączące sygnały przesyłane od ONU do OLT. Urządzenia rozgałęziające są zazwyczaj dostępne ze współczynnikiem podziału 1:n lub 2:n.

Aby poprawić efektywność oraz niezawodność sieci (np. wejście dla dodatkowych sygnałów, punkty służące monitorowaniu sieci, zabezpieczenie sieci przez zastosowanie różnych ścieżek), można zastosować urządzenie ze stosunkiem podziału h:n, gdzie $1<h<n$.

Zazwyczaj urządzenia rozgałęziające stosowane w sieci ODN o architekturze drzewa są symetryczne. Oznacza to, że tłumienie sygnału optycznego wchodzącego na dowolny port wejściowy w stosunku do dowolnego portu wyjściowego jest takie samo dla dowolnej pary portów wejściowych i wyjściowych. Te wymagania wynikają

głównie z potrzeby uproszczenia reguł zarządzania budżetem mocy sygnału optycznego w ODN oraz ogólnym uproszczeniem metod projektowania sieci.

Konfiguracja punkt - punkt (rysunek 8.4), kiedy jedno ONU jest połączone z OLT poprzez sieć ODN można traktować jako specyficzne zastosowanie architektury punkt - wielopunkt. W tym przypadku nie występują optyczne urządzenia rozgałęziające w sieci ODN. Dowolne ONU połączone jest z OLT za pomocą jednego lub dwóch dedykowanych włókien światłowodowych. Konfigurację tę określa się mianem pojedynczej gwiazdy. Umożliwia ona użycie włókien światłowodowych o maksymalnej długości pomiędzy OLT a dowolnym ONU, zwiększając zasięg sieci w stosunku do rozwiązania wykorzystującego architekturę drzewa.



Rysunek 8.4 Schemat architektury typu gwiazda

Funkcje sieci ODN

Optyczną sieć dystrybucyjną opisują następujące właściwości:

- bezpośrednie połączenie optyczne - sieć ODN zapewnia bezpośrednią wymianę sygnałów optycznych pomiędzy OLT i ONU. W przypadku architektury punkt-punkt cecha ta jest naturalna z powodu braku urządzeń rozgałęziających;
- rozgałęzianie i łączenie sygnałów optycznych - rozgałęzianie sygnału optycznego jest realizowane na strumieniu wychodzącym z OLT (strumień w „dół"), zaś łączenie wykonywane jest na strumieniach wychodzących od poszczególnych ONU (strumień w „górę"). Funkcje te są realizowane za pomocą optycznych urządzeń rozgałęziających;
- możliwość przesyłania sygnałów optycznych o różnych długościach fali - równoczesna transmisja sygnałów optycznych o różnych długościach fali w obydwu kierunkach (od i do abonenta) w jednym włóknie światłowodowym;
- monitorowanie pracy sieci - sieć ODN powinna mieć możliwość podłączenia urządzeń kontrolno-pomiarowych służących do monitorowania jej pracy. Działanie tych urządzeń nie może zakłócać pracy samej sieci. Punkty dostępu mogą być umieszczone przy OLT, jednostkach ONU bądź w dowolnym miejscu sieci ODN. Punkty dostępu powinny umożliwiać dołączenie np. reflektometrów czy mierników poziomu mocy;
- Interfejsy optyczne - ODN musi posiadać fizyczne interfejsy optyczne umożliwiające podłączenie do niego urządzeń OLT i ONU.

W sieci ODN zalecana jest praca w oknach 1310nm lub/i 1550nm. Oznacza to, że wykorzystując okno 1310nm sieć powinna umożliwić przesyłanie sygnałów optycznych

z zakresu 1260nm do 1360nm. W oknie 1550nm przedział dopuszczalnych długości fal świetlnych wynosi od 1480nm do 1580nm. W razie zastosowania wzmacniaczy optycznych przedział długości fal może być zawężony.

8.3 Wymagania dotyczące urządzeń stosowanych w sieciach dostępowych

Istnieje bardzo wiele rozwiązań systemowych spotykanych w sieciach dostępowych. Z tego względu urządzenia w nich stosowane muszą się charakteryzować dużą elastycznością i pozwalać na realizację zróżnicowanych potrzeb. Wymagania takie spełniają konstrukcje modułowe oparte na:

- kartach rozpoczynających pracę bezpośrednio po ich umieszczeniu w urządzeniu,
- blokowej strukturze oprogramowania,
- dużej elastyczności konfiguracji.

Rozwiązania tego typu umożliwiają operatorowi sieci dostępowej szybkie udostępnienie nowych funkcji, które będą się pojawiać wraz z rozwojem usług.

Systemy dostępowe powinny ponadto charakteryzować się odpowiednimi parametrami technicznymi. Powinny posiadać:

- odpowiednie styki elektryczne i optyczne od strony sieci teletransmisyjnej zgodne z wymaganiami systemów PDH (2, 34, 140 Mbit/s) i SDH (155, 622 Mbit/s),
- odpowiednie styki elektryczne i optyczne od strony sieci dostępowej (styki aplikacyjne) zgodne z:
  - wymaganiami sieci pasywnych PON,
  - wymaganiami sieci aktywnych AON,
  - strukturami typu punkt-punkt,

a dokładnie powinny być wyposażone w następujące interfejsy aplikacyjne (tabela 8.1):
a ponadto powinny posiadać:

- możliwość implementacji styków dla sieci szerokopasmowych VB5.1,VB5.2,
- możliwość implementacji styków dla sieci ATM,
- obiektowo zorientowane oprogramowanie,
- wysokie parametry niezawodnościowe,
- układy przełączania i konsolidacji ruchu dla wąskopasmowych usług komutowanych i niekomutowanych.

Tabela 8.1 Interfejsy aplikacyjne w urządzeniach dostępowych

E1	G.703/G.704	2Mbit/s	kod HDB3
interfejs optyczny		8Mbit/s	
interfejs HDSL	2/3 pary		kod 2B1Q lub CAP
U			kod 2B1Q
V.35		n x 64 kbit/s	
V.11		n x 64 kbit/s	
V.24			
V.24/V.28			
X.24/V.11			
64kbit/s	G.703		
BRA	(ISDN)		kod na styku U 2B1Q
PRA (ISDN)			
V.5.1, V.5.2.			
Z (POTS)			
interfejsy analogowe 2/4 wr sygnalizacja E&M (ważna jest możliwość ustawienia poziomów sygnałów w ramach ustawień systemowych)			
oraz interfejsy systemu zarządzania: – V.24 RS 232, Q1, Q3 do TMN, F			

Usługi w sieciach dostępowych

Usługi podstawowe w sieciach dostępowych.

Do podstawowych usług telekomunikacyjnych w systemie dostępu abonenckiego należą:

- telefonia o standardowym paśmie (300 Hz - 3.4 kHz),
- transmisja telefaksowa (grupy 3),
- transmisja danych przy użyciu modemu,
- realizacja połączeń z aparatu samoinkasującego.

Jako urządzenie końcowe, dołączane do interfejsu abonenckiego **Z** może w tym wypadku służyć standardowy analogowy aparat telefoniczny, aparat samoinkasujący, telefaks grupy 3 lub modem.

W telefonicznej sieci dostępu abonenckiego połączenia pomiędzy centralą końcową a abonenckimi aparatami telefonicznymi, tradycyjnie realizowane w paśmie naturalnym, przy pomocy miedzianych kabli symetrycznych, zostają zastąpione przez rozwiązania korzystające z transmisji cyfrowej w trakcie światłowodowym na całej drodze od centrali lokalnej do abonenta lub na jej części. Podstawowe założenia dotyczące własności systemu dostępu abonenckiego to:

- zapewnienie parametrów jakościowych transmisji i dostępności usług (w tym również przewidywanych do wprowadzenia w przyszłości) takich jak dla abonentów dołączonych do centrali w sposób konwencjonalny,
- pełna przezroczystość łącza abonenckiego z punktu widzenia urządzenia końcowego, pozwalająca na użytkowanie typowych dla rozdzielczej sieci kablowej abonenckich aparatów telefonicznych, a w wypadku połączenia analogowego pomiędzy systemem dostępowym i centralą lokalna również z punktu widzenia centrali,
- sposób korzystania przez użytkownika z usług w sieci dostępowej nie różniący się od tego jaki występuje w publicznej sieci telefonicznej.

Jako interfejs abonencki w sieci dostępowej jest rozpatrywany interfejs kanału telefonicznego pomiędzy wyposażeniem abonenckim w optycznym module sieciowym (ONU) i terminalem abonenckim - standardowym aparatem telefonicznym. Własności interfejsu są uzależnione od usług udostępnianych użytkownikowi. W wypadku

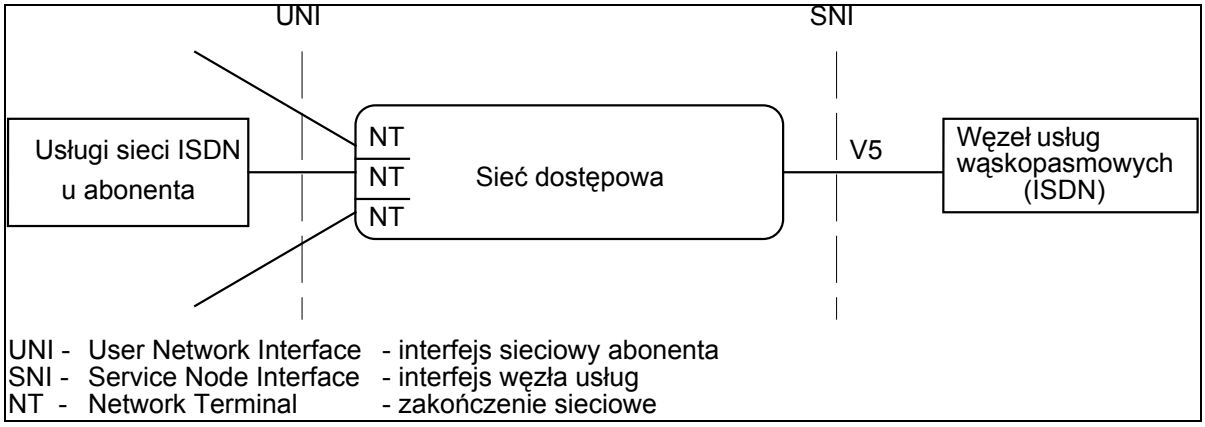
stosowania znormalizowanego urządzenia końcowego (terminala) w postaci analogowego aparatu telefonicznego wymagane parametry mogą być określane analogicznie jak w wypadku dostępu do przewodowej publicznej telefonicznej sieci komutowanej (PSTN).

W tym wypadku można opierać się na zaleceniach ITU-T dla interfejsu Z (Zal. Q.552). Interfejs Z występuje dla połączenia analogowych linii abonenckich i przenosi sygnały takie jak mowa, dane w paśmie kanału telefonicznego (transmisja modemowa), sygnały DTMF z klawiatury itp. Dodatkowo interfejs Z powinien zapewniać:

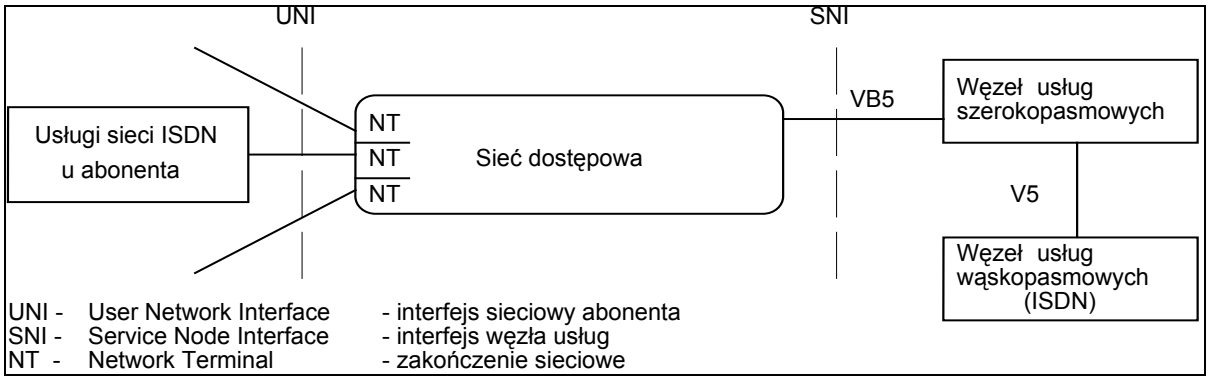
- zasilanie stałoprądowe terminala abonenckiego,
- możliwość przesyłania sygnałów sygnalizacji przewidzianych dla abonenckiego łącza naturalnego, w tym:
  - sygnałów wybierczych (dekadowe i wieloczęstotliwościowe DTMF) w celu zestawienia połączenia lub realizacji dodatkowych usług abonenckich,
  - sygnałów liniowych przenoszących informacje o wzięciu do pracy i zakończeniu połączenia,
  - sygnał wywołania abonenta żądanego,
  - sygnałów zaliczania w celu informowania abonenta o opłacie za połączenie,
  - sygnałów tonowych i zapowiedzi słownych,
  - sygnałów przywołania sterowania dla powiadomienia centrali, że abonent chce nadać rozkaz komutacyjny w fazie rozmowy.

Usługi ISDN w sieciach dostępowych

Zgodnie ze schematem funkcjonalnym sieci dostępowej, oparte na blokach zdefiniowane w zaleceniu ITU-T G.902, wyróżniono dwa typy interfejsów od strony abonenta UNI (*ang. User Network Interface*) i od strony węzłów usługowych SNI (*ang. Service Node Interface*).



Rysunek 8.5 Sieć dostępowa dołączona do węzła usługowego (ISDN) poprzez interfejs V5



Rysunek 8.6 Sieć dostępowa dołączona do węzła usługowego (ISDN) poprzez interfejs VB5

W sieciach dostępowych stosuje się dwie topologie umożliwiające realizację usług wąskopasmowych (w tym ISDN):

- sieć dostępowa dołączona do węzła usługowego poprzez interfejsy V5 (rysunek 8.5),
- sieć dostępowa dołączona do węzła usługowego przez interfejs VB5 - w tym przypadku usługi wąskopasmowe są realizowane jako podzbiór usług szerokopasmowych (rysunek 8.6).

Usługi oferowane w sieciach ISDN zostały podzielone na dwie grupy:

- usługi przenoszenia (*ang. bearer services*),
- teleusługi (*ang. teleservices*).

Grupy powyższe zostały podzielone na dwie podgrupy usług podstawowych i dodatkowych. Usługi podstawowe realizują typowe zadania a usługi dodatkowe modyfikują je, rozszerzając ich właściwości. Tak, więc usługi dodatkowe mogą być oferowane tylko z usługami podstawowymi, których dotyczą. Należy też dodać, że jedna usługa dodatkowa może modyfikować kilka usług podstawowych.

Usługi przenoszenia związane są z przesyłaniem informacji i realizują funkcje trzech najniższych warstw modelu odniesienia. Usługi te realizowane są przez sieć ISDN.

Teleusługi związane są ze wszystkimi warstwami modelu odniesienia. Realizowane są przez sieć ISDN, jak również terminale końcowe użytkownika. Oferowane są one w punkcie styku terminala końcowego użytkownika. Związane są, więc nie tylko z właściwościami sieci, lecz również z możliwościami terminala końcowego użytkownika. Usługi warstw wyższych (4-7) mogą nie występować w sieci ISDN, lecz mogą wymagać obsługi przez urządzenia końcowe użytkownika, gdyż ich protokoły są przekazywane w sposób przezroczysty przez sieć. W przypadku konieczności konwersji protokołów określonych teleusług (zmiana protokołu przy przejściach z jednej do drugiej sieci - np. dostęp do Internetu poprzez określoną aplikację ISDN, konwersja prędkości transmisji, itp.), sieć ISDN musi obsługiwać funkcje warstw wyższych.

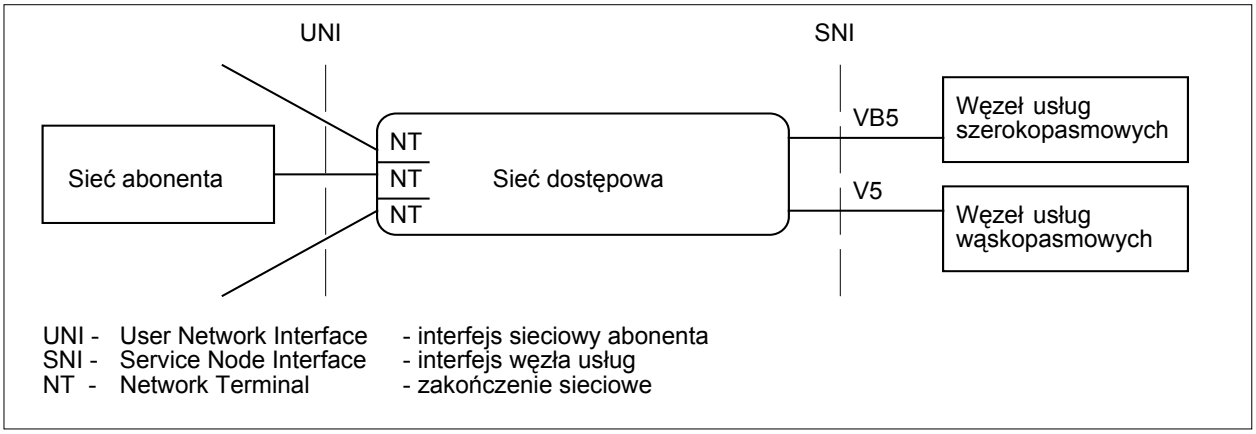
Usługi szybkiej transmisji danych w sieciach dostępowych

Usługi szybkiej transmisji danych leżą u podstaw koncepcji sieci dostępowych. Szerokopasmowa sieć dostępowa jest platformą dla dostarczenia pełnego zakresu nowych usług. Lista możliwych usług zmienia się z upływem czasu. Często pojawiają się nowe usługi a niektóre nie znajdują odbiorców. Dlatego można przedstawić jedynie przykładową listę usług:

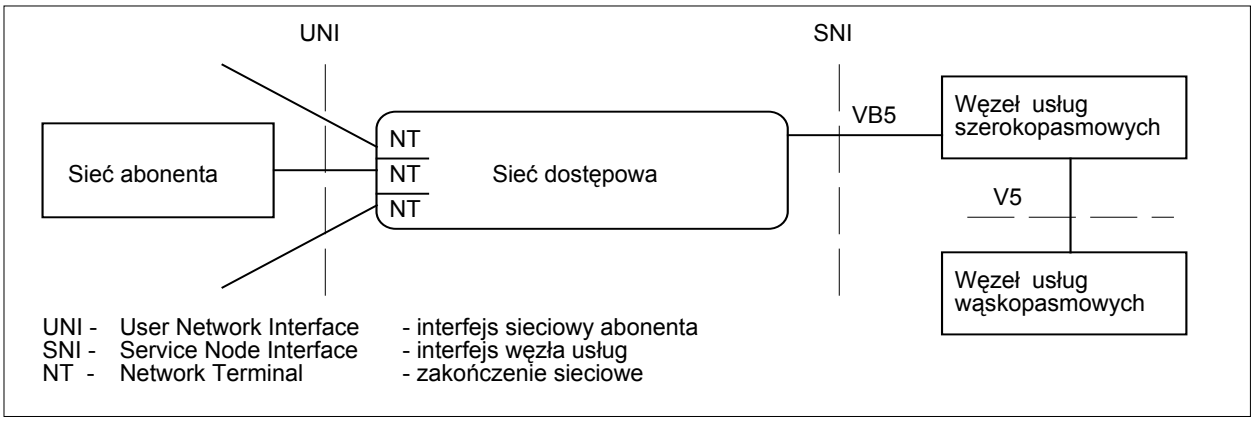
- informacja na życzenie (*ang. Information on Demand*),
- edukacja,

– usługi na życzenie (*ang. Service on Demand*),
– telepraca,
– transfer plików,
– łączenie sieci LAN.

Punktem wyjścia w opisie parametrów sieci dostępowej może być przyjęty schemat funkcjonalny sieci złożony z bloków zdefiniowanych w zaleceniu ITU-T G.902, który obejmuje szeroką gamę usług. W sieci dostępowej wyróżnione są dwa typy interfejsów od strony abonenta UNI (*ang. User Network Interface*) i od strony węzłów usługowych SNI (*ang. Service Node Interface*) (rysunek 8.7, rysunek 8.8).



Rysunek 8.7 Sieć dostępowa dołączona do węzła usług przez interfejsy V5 i VB5



Rysunek 8.8 Sieć dostępowa dołączona do węzła usług przez interfejs VB5

Wyróżniamy dwie klasy usług szybkiej transmisji danych w sieciach dostępowych :
– łącza cyfrowe o przepływnościach do 2 Mb/s do transmisji danych (np. z protokołami Frame Relay, PPP),
– łącza cyfrowe o przepływnościach od 2 Mb/s pracujące z protokołem ATM.

Łącza cyfrowe o przepływności do 2 Mb/s są wykorzystywane do realizacji sieci pakietowych. Tego typu łącza służą jako dostęp do Internetu, wykorzystywane są do połączeń w sieciach korporacyjnych. Najczęściej w warstwie liniowej (zgodnie z modelem odniesienia dla systemów otwartych ISO OSI) używane są protokoły Frame Relay i PPP (*ang. Point to Point Protocol*). W warstwie sieciowej podstawowym protokołem jest IP (*ang. Internet Protocol*). Stosowane są różnego typu interfejsy takie

jak V.35, V.36, X.21, V.24, G.703. Terminalami w sieciach pakietowych są routery, komputery, przełączniki pakietów.

Łącza cyfrowe o przepływnościach od 2 Mb/s pracujące z protokołem ATM mogą być wykorzystywane do przenoszenia usług w kanałach wirtualnych VC (*ang. Virtual Channel*) i ścieżkach wirtualnych VP (*ang. Virtual Path*). Tego typu łącza są postrzegane jako docelowa platforma służąca realizacji usług w sieci szerokopasmowej. Wyróżnia się następujące kategorie usług:

- **CBR** (*ang. Constant Bit Rate*) - odnosi się do usług charakteryzujących się stałym zapotrzebowaniem na pasmo takich jak emulacja łączy (*ang. circuit emulation*), transmisja głosu bez kompresji i mechanizmu wykrywania ciszy (*ang. silence removal*),
- **VBR** (*ang. Variable Bit Rate*) - odnosi się do usług generujących strumień danych o zmiennej przepustowości. Jest to klasa, która pozwala naadaptację do wymagań na parametry strumienia danych dla realizowanych usług. Wyróżnia się dwie podklasy:
  - rt-VBR (*ang. real time VBR*), w której można oszczędnie operować pasmem poprzez multipleksację statystyczną. Tą klasę można stosować dla źródeł ruchu o nierównomiernym strumieniu,
  - nrt-VBR (*ang. non-real time VBR*) która nie jest zależna od czasu. Jest stosowana do usług wymagających szybkiej reakcji, lecz nie generujących ruchu o mocno zmiennym strumieniu (np. transakcje bankowe, systemy nadzoru),
- **ABR** (*ang. Available Bit Rate*) - odnosi się do usług bez istotnych wymagań czasowych z zachowaniem możliwości zagwarantowania w ograniczonym zakresie sprawiedliwego podziału pasma. Kryterium podziału pasma jest dopuszczalny poziom traconych komórek,
- **UBR** (*ang. Unspecified Bit Rate*) - odnosi się do usług bez jakiejkolwiek gwarancji jakości dla transmisji informacji nie wymagającej określenia dopuszczalnych poziomów opóźnienia lub fluktuacji opóźnienia.

Terminalami dla tych kategorii usług mogą być dowolne urządzenia z interfejsem ATM. Typowe terminale to: routery, komputery, przełączniki ATM, przełączniki Ethernet, urządzenia do transmisji i odbioru wizji i fonii. Obecnie najwięcej zastosowań protokołu ATM jest związanych z przenoszeniem protokołów lokalnych sieci komputerowych i Internetu. Istnieje szereg zdefiniowanych przez ATM Forum, ETSI i ITU-T interfejsów sieciowych abonenta. Obejmują one kanału przepustowości od 2 Mb/s do 2,4 Gb/s. W sieciach dostępowych zalecane są interfejsy ATM 2 i 25 Mb/s dla interfejsów elektrycznych i 155, 622 Mb/s dla interfejsów optycznych.

Usługi transmisji sygnałów telewizyjnych i radiofonicznych

Podstawową usługą szerokopasmową jest dostarczenie abonentom programów telewizyjnych i radiofonicznych pochodzących z różnych źródeł (stacje naziemne, satelitarne, lokalne studia itp.). W sieci może być transmitowanych kilkadziesiąt kanałów telewizyjnych (dla standardu D/K do 90 kanałów). Nowe możliwości wiążą się z wprowadzeniem kanału zwrotnego umożliwiającego takie usługi jak:

- nadzór wizyjny nad obiektami,
- monitorowanie stanu pacjentów tzw. „wideo-medycyna”,
- „wideo-zakupy” itp.

W najbliższych latach należy liczyć się z rozwojem takich usług szerokopasmowych jak:
- filmy na życzenie,
- telewizja interaktywna,
- interaktywne gry wideo,
- biblioteki multimedialne,
- wideotelefon itp.

8.4 Stan normalizacji dla szerokopasmowych sieci dostępowych

W Europie prowadzone są równolegle liczne prace standaryzacyjne w kierunku specyfikacji systemu FITL. Do głównych organizacji zajmujących się tą dziedziną należy zaliczyć Europejski Instytut Standardów Telekomunikacyjnych ETSI, który podjął prace w kierunku znormalizowania optycznych sieci dostępowych OAN. Rezultatami tych oraz wcześniejszych prac związanych z zagadnieniami systemu FITL są między innymi następujące dokumenty:

- prETS 300 463 Transmission and Multiplexing; The requirements of optical access networks OAN to provide services based on 64kb/s bearer capabilities,
- prETS 300 681 Transmission and Multiplexing; Optical Distribution Network ODN for OAN,
- prETS 300 781 Transmission and Multiplexing; Functional and system parameters,
- ETS 300 019 Equipment Engineering; Environmental conditions and environmental tests for telecommunications equipment
- ETS 300 324 Transmission and Multiplexing; V.5.1 interface specification for the support of access network.

Innym ważnym europejskim ciałem standaryzacyjnym jest grupa EURESCOM, która opracowała w ramach projektu P 306 poradnik techniczny obejmujący zagadnienia ściśle związane z systemami sieci dostępowych, a szczególnie sieciami FITL. Rezultatem prac tej organizacji są między innymi następujące dokumenty:
- Technical Advisory on FITL equipment for Passive Optical Networks,
- Strategic recommendations for FITL systems,
- Operation of FITL systems.

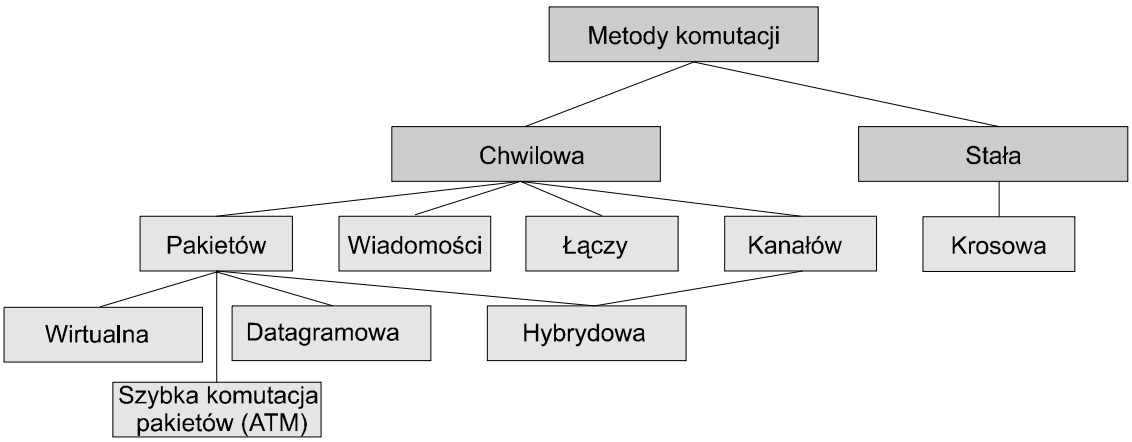
Równolegle z europejskimi podobne prace standaryzacyjne prowadzone są w Stanach Zjednoczonych w Labolatoriach Bella. Organizacją wydającą odpowiednie standardy amerykańskie jest BellCore, a dokumentem definiującym i opisującym systemy FITL jest TA-NWT-000909: Generic Requirements and Objectives Fiber In The Loop Systems.

9 Komutacja wiadomości w sieciach telekomunikacyjnych

Sieci telekomunikacyjne posługują się różnymi technikami komutacji wiadomości. W starszych sieciach technika komutacji silnie zależy od realizowanych w sieci usług. W najnowszych rozwiązaniach można zauważyć działania mające na celu uniezależnienie techniki komutacji wiadomości od realizowanych usług. Takim przykładem może być asynchroniczny tryb transferu (to rozwiązanie ATM, które nie korzysta z sieci transmisyjnej synchronicznej SDH).

Optymalizacją technik komutacji wiadomości w sieci zainteresowani są zarówno producenci sprzętu telekomunikacyjnego, jak i jego operatorzy. Optymalizacja dotyczy współczynników technicznych charakteryzujących sieć (jakości świadczenia usług, przepustowości i jej efektywnego wykorzystania itp.) jak i jej parametrów ekonomicznych (koszty budowy sieci, koszty jej utrzymania, rozbudowy i ewolucji). Zwykle, choć nie zawsze, parametry ekonomiczne mają większe znaczenia dla operatorów.

Na rysunku 9.1 zamieszczono klasyfikacje metod komutacji wiadomości w sieci.



Rysunek 9.1 Metody komutacji stosowane w sieciach telekomunikacyjnych

Proces dostarczania informacji użytkownikowi od jej źródła można rozbić na następujące etapy:

- dostarczenie informacji do punktu wprowadzania do sieci (źródło wiadomości - urządzenie końcowe);
- formowanie informacji w postać wiadomości i wprowadzenie jej do sieci;
- nadawanie (bezpośrednie lub z zapamiętywaniem i/lub przetwarzanie);
- wyprowadzanie wiadomości z sieci w postaci przydatnej do dalszego wykorzystania;
- dostarczenie wiadomości do miejsca wykorzystania - użytkownika.

W punktach wprowadzania i wyprowadzania i niekiedy w punktach pośrednich może zachodzić zapamiętywanie całej wiadomości lub tylko jej adresu i numeru (lub innych danych służbowych niezbędnych w procesie przesyłania).

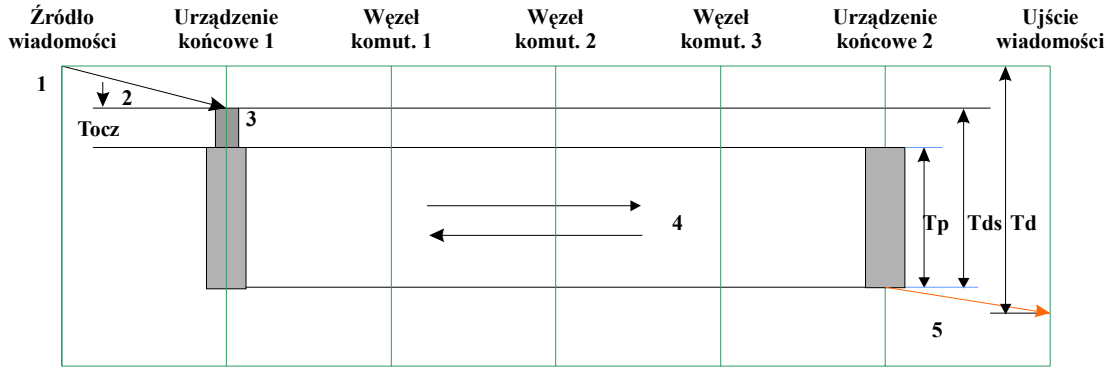
Można w chwili obecnej wyróżnić 3 podstawowe metody dostarczania informacji w postaci wiadomości przesyłanej w sieci (od punktu wprowadzania do punktu wyprowadzania):

- przez kanały zestawione, skrosowane na stałe;
- przez kanały zestawione w węzłach komutacyjnych na czas trwania jednej usługi;
- sztafetowe przekazywanie od jednego węzła do następnego z zapamiętaniem wiadomości w każdym węźle komutacyjnym i nadawaniem do następnego (w odpowiednim kierunku) w miarę istnienia wolnych kanałów do tego węzła sieci.

9.1 Komutacja krosowa

Komutacja krosowa jest przykładem komutacji stałej. Kanały pomiędzy abonentami są galwanicznie ze sobą łączone na danej trasie. Tak zestawione kanały łączą na stałe lub wg harmonogramu czasowego urządzenie końcowe wejściowe z urządzeniem końcowym wyjściowym.

Kanały zestawione metodą komutacji krosowej zapewniają najszybsze przesyłanie wiadomości (rysunek 9.2) ponieważ wykluczone jest oczekiwanie na jego zwolnienie (gdy UK jest wolne to kanały też są wolne) nie jest też wymagane adresowanie, które znacznie komplikuje protokoły komunikacyjne. Jednak to rozwiązanie nie jest ekonomiczne, ponieważ w momentach ciszy w medium brak jest możliwości multipleksacji w kanale wiadomości pochodzących od dodatkowych połączeń abonenckich.



LEGENDA

1. Powstanie zgłoszenia
2. Dostarczenie zgłoszenia do UK
3. Oczekiwanie na zezwolenie UK na wprowadzania Wiadomości
4. Wymiana wiadomości
5. Dostarczenie wiadomości do urządzenia końcowego

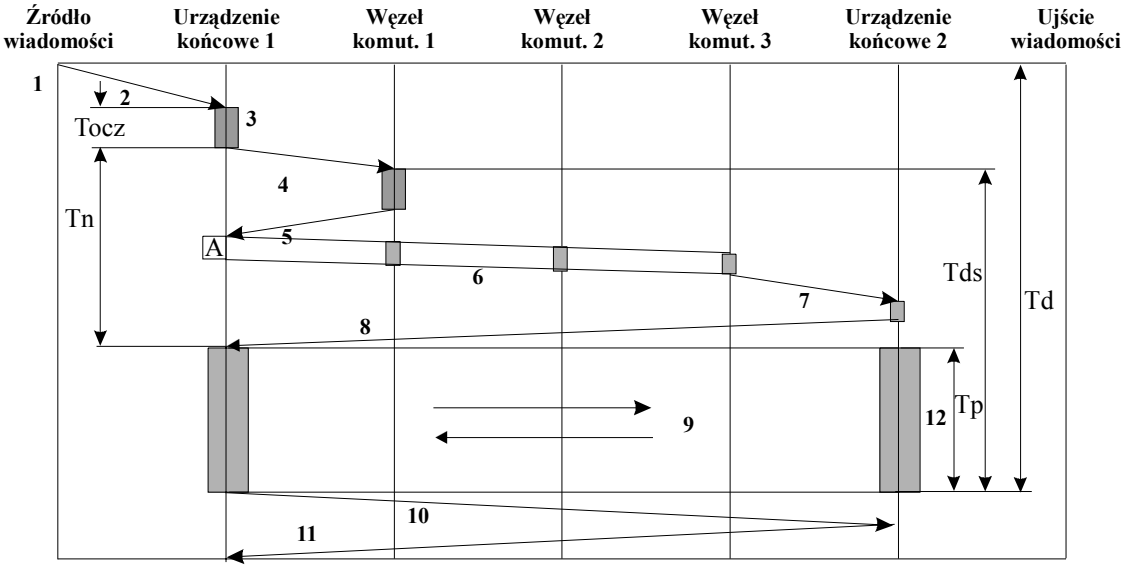
Tocz- czas oczekiwania na zwolnienie ujścia wiadomości
Tp- czas transmisji
Tds- czas wymiany wiadomości pomiędzy urządzeniami Końcowymi
Td- czas dostarczenia wiadomości do ujścia

Rysunek 9.2 Komutacja krosowa

9.2 Komutacja kanałów

W metodzie tej w systemie sygnalizacyjnym (na podstawie nadanego adresu urządzenia końcowego wywoływanego) realizowany jest proces zestawiania drogi połączeniowej pomiędzy abonentami. W procesie łączenia wykorzystywane są wolne kanały, tzn. te, które nie wchodzą w skład drogi połączeniowej w innej relacji. Organizacja połączenia pomiędzy źródłem wiadomości i jej ujściem do sieci może być jednokierunkowa (simpleks) lub dwukierunkowa (dupleks). Zestawione połączenie funkcjonuje na czas realizacji jednej usługi (np. jednej rozmowy). Wiadomość jest nadawana jednocześnie we wszystkich kanałach wchodzących w skład drogi połączeniowej. Powinny one posiadać jednakową zdolność przepustową, chociaż

systemy transmisji (modulacji) mogą być inne. Przykład procesów wymiany informacji w metodzie komutacji kanałów przedstawiono na rysunku 9.3.



LEGENDA

1. Powstanie zgłoszenia
2. Dostarczenie zgłoszenia do UK
3. Oczekiwanie na zezwolenie UK na wprowadzanie wiadomości
4. Zapotrzebowanie na obsługę zgłaszane do węzła sieci telekomunikacyjnej
5. Przyjęcie zapotrzebowania
6. Przekazanie adresu i zestawienie połączenia
7. Wywołanie abonenta i oczekiwanie na odpowiedź
8. Zgłoszenie abonenta oddalonego
9. Wymiana wiadomości
10. Przekazanie sygnału rozłączenia i zwolnienia oraz Zwolnienie kanału
11. Przekazanie sygnału rozłączenia i zwolnienia oraz zwolnienie kanału
12. Dostarczenie wiadomości do urządzenia końcowego
Tocz- czas oczekiwania na zwolnienie ujścia wiadomości
Tp - czas transmisji
Tds - czas wymiany wiadomości pomiędzy urządzeniami końcowymi
Td - czas dostarczenia wiadomości do ujścia
Tn - czas realizacji procesów sygnalizacyjnych

Rysunek 9.3 Komutacja kanałów

Zestawianie drogi między urządzeniami końcowymi jest dokonywane w węzłach komutacyjnych sieci w ślad za nadanym adresem (np. nr abonenta docelowego). Wiadomość może być nadana dopiero po całkowitym zestawieniu drogi. W procesie zestawiania drogi połączeniowej może się zdarzyć, że wystąpi brak wolnych kanałów w danej części drogi lub zajęty będzie jeden z węzłów komutacyjnych pośredniczących. Wówczas w systemach telekomunikacyjnych z oczekiwaniem (kolejkowaniem zgłoszeń) urządzenie końcowe 1 będzie oczekiwać na zwolnienie się danego zasobu (węzła komutacyjnego) lub kanału. W systemach bez oczekiwania urządzenie końcowe 1 otrzyma sygnał o niemożności zestawienia połączenia oraz sygnał o braku możliwości realizacji usługi.

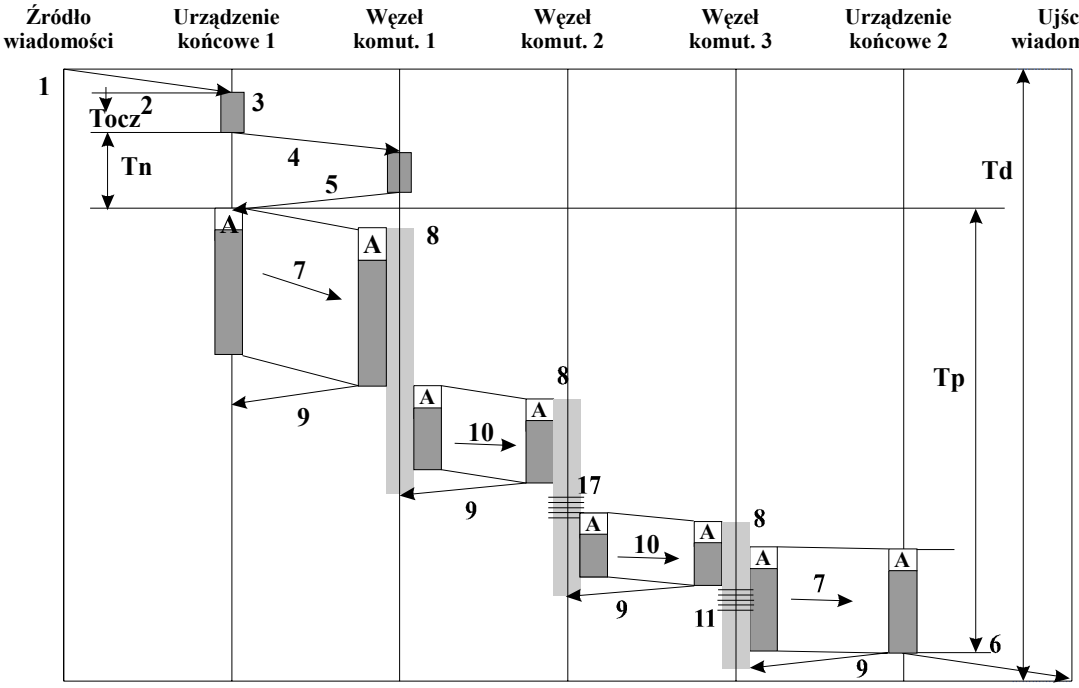
W obu przypadkach mamy do czynienia z powstaniem opóźnienia w dostarczeniu wiadomości oraz zbyteczne zajmowanie kanałów i wyposażenia węzłów komutacyjnych w przypadku braku możliwości realizacji usługi.

Ponadto, nawet gdy zestawione zostanie połączenie, to usługa może być niezrealizowana, np. ze względu na nieobecność adresata.

9.3 Komutacja wiadomości

Urządzenia końcowe ma bezpośrednie (stałe) połączenie ze swoim (może ich być więcej niż jeden) węzłów komutacyjnym (rysunek 9.4). Jeżeli urządzenie końcowe 1

jest wolne, wiadomość łącznie z adresem nadawana jest do najbliższego (ze względu na kierunek) węzła komutacyjnego, gdzie jest ona zapisywana w kolejce (buforze wyjściowym) do następnego węzła komutacyjnego (zgodnie z adresem na podstawie tablicy marszrutyzacji węzła). Po zwolnieniu się kanału do następnego węzła komutacyjnego wiadomość jest nadawana. W węźle następnym jest ona zapamiętana i zgodnie z adresem ponownie ustawiana w kolejce do następnego węzła komutacyjnego. Proces ten jest powtarzany aż do osiągnięcia węzła komutacyjnego adresata, który następnie przesyła informację do urządzenia końcowego.



LEGENDA

1. Powstanie zgłoszenia
2. Dostarczenie zgłoszenia do UK
3. Oczekiwanie na zezwolenie UK na wprowadzanie wiadomości
4. Zapotrzebowanie na obsługę zgłaszane do węzła sieci telekomunikacyjnej
5. Przyjęcie zapotrzebowania
6. Dostarczenie wiadomości do urządzenia końcowego
7. Transmisja wiadomości z małą szybkością
8. Zapis i przetwarzanie wiadomości
9. Potwierdzenie poprawnego odbioru
10. Transmisja wiadomości z dużą szybkością
11. Przetwarzanie wiadomości

Tocz- czas oczekiwania na zwolnienie ujścia wiadomości
Tp - czas transmisji
Td - czas wymiany wiadomości pomiędzy urządzeniami końcowymi
Tn - czas zestawiania połączenia

Rysunek 9.4 Komutacja wiadomości

Na każdym węźle oprócz operacji wcześniej wymienionych realizowana jest kontrola poprawności odebranych informacji a następnie:

- gdy odebrana wiadomość jest poprawna węzeł komutacyjny, który odebrał informację wysyła potwierdzenie odbioru;
- gdy wiadomość jest odebrana błędnie, wysyłane jest żądanie powtórzenia wiadomości;

W każdym węźle wiadomość może być przechowywana określony czas (np. celem kontroli).

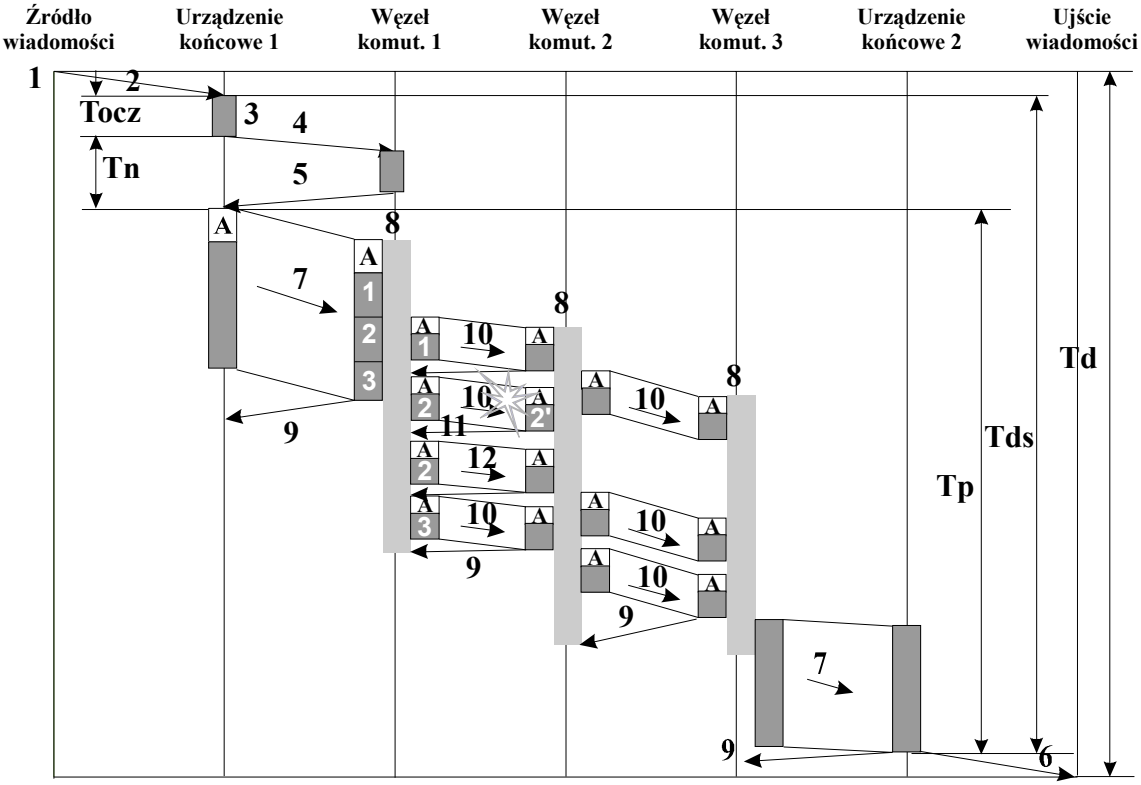
W trakcie komutacji wiadomości nie zestawia się wcześniej drogi. W danym momencie zajmuje się tylko jeden kanał składowy między węzłami komutacyjnymi sąsiednimi (może być na drodze bezpośredniej lub obejściowej wg algorytmu marszrutyzacji). Pozwala to na lepsze wykorzystanie kanałów. Zabezpiecza także

przekazywanie wiadomości między urządzeniami, które nie muszą pracować w tym samym czasie i mogą pracować z różnymi szybkościami oraz różnymi kodami. Dopasowanie zachodzi w węźle komutacyjnym, który ma bezpośrednie połączenie do urządzenia końcowego 2.

Wadą tego sposobu są ograniczone możliwości realizacji usług zależnych czasowo np. transmisji mowy (zmienne opóźnienia w transmisji pomiędzy węzłami komutacyjnymi).

9.4 Komutacja pakietów

Cała wiadomość do przesłania dzielona jest w pierwszym węźle komutacyjnym na części o jednakowej długości zwane pakietami (rysunek 9.5). Każdy z pakietów zaopatrzony jest w adres odbiorcy i nadawcy. Proces podziału wiadomości na pakiety może być również realizowany w urządzeniu końcowym.



LEGENDA

1. Powstanie zgłoszenia
2. Dostarczenie zgłoszenia do UK
3. Oczekiwanie na zezwolenie UK na wprowadzanie wiadomości
4. Zapotrzebowanie na obsługę zgłaszane do węzła sieci telekomunikacyjnej
5. Przyjęcie zapotrzebowania
6. Dostarczenie wiadomości do urządzenia końcowego
7. Transmisja
8. Zapis i przetwarzanie wiadomości
9. Potwierdzenie poprawnego odbioru
10. Transmisja pakietu
11. Zapotrzebowanie na powtórne przesłanie
12. Powtórna transmisja pakietu

Tocz - czas oczekiwania na zwolnienie ujścia wiadomości
Tp - czas transmisji
Tds - czas wymiany wiadomości pomiędzy urządzeniami końcowymi
Td - czas dostarczenia wiadomości do ujścia
Tn - czas zestawiania połączenia

Rysunek 9.5 Komutacja pakietów

Pakiety są nadawane pojedynczo. W miejscu przeznaczenia (WS, do którego podłączone jest urządzenie końcowe odbiorcy) pakiety zostają połączone w sposób uporządkowany w wiadomość.

Wyróżniamy dwie metody obróbki pakietów informacyjnych w sieci z komutacją pakietową, są to:
- komutacja datagramowa;
- komutacja wirtualna.

Komutacja datagramowa

W tym przypadku nie istnieją procesy: zestawiania drogi połączeniowej i rozłączania. Sieć przyjmuje pakiet z wiadomością (który zawiera pełny adres abonenta docelowego) a następnie kieruje go od węzła do węzła w kierunku abonenta końcowego. W urządzeniu końcowym abonenta docelowego realizowany jest proces scalania pakietów w całą wiadomość.

Komutacja wirtualna

Na etapie zestawiania połączenia wirtualnego (na podstawie sygnalizacji w sieci) dla zadanego adresu odbiorcy wybierana jest droga, po której będzie przesyłany pakiet do urządzenia końcowego 2. Z punktu widzenia abonentów sieci droga komutacji pakietów widziana jest jakby była zestawiona, czyli jakby istniało bezpośrednie połączenie (pomiędzy abonentami), chociaż fizycznie takiej drogi nie ma. W większości przypadków sieć powinna zabezpieczyć odpowiednią kolejność przybywania pakietów do miejsca przeznaczenia.

Niewątpliwą zaletą komutacji wirtualnej jest to, iż wykorzystuje fizyczne połączenie jedynie na czas transmisji wiadomości. Ponadto między urządzeniami końcowymi można zestawiać wiele połączeń wirtualnych jednocześnie.

W metodzie komutacji pakietów sieć jest odpowiedzialna za bezbłędną transmisję pakietów (choć nie zawsze, np. w Frame Relay czy ATM nie). To zadanie realizowane jest w węzłach sieci, które przechowują kopię pakietu do momentu aż następny węzeł potwierdzi jego bezbłędne przyjęcie. Natomiast pakiety niepotwierdzone są powtórnie nadawane. Stąd wniosek, że pakiet musi podlegać kodowaniu nadmiarowemu. Polega to na dodaniu wg określonego algorytmu nadmiaru (np. sumy kontrolnej), który w węzłach komutacyjnych wykorzystywany jest do detekcji błędów (rzadziej do detekcji i korekcji błędów).

10 Symulacja systemów i sieci telekomunikacyjnych

10.1 Metody badań systemów i sieci telekomunikacyjnych

Metody badań wykorzystywane w procesie projektowania i analizy systemów łączności:

- **analityczne**, polegają na opisie matematycznym funkcjonowania systemu łączności. Stosuje się wówczas, gdy potrafimy ująć oraz wyznaczyć ilościowe i jakościowe związki pomiędzy interesującymi nas wielkościami. Na podstawie wyników z modelu matematycznego wnioskuje się o pracy badanego systemu rzeczywistego.
- **symulacyjne**, polegają na odwzorowaniu funkcjonowania badanego systemu z zastosowaniem odpowiedniego oprogramowania komputerowego. Odwzorowanie realizowane jest z określoną dokładnością (adekwatnością). Na podstawie zjawisk zachodzących w modelu badanego systemu wnioskuje się o pracy badanego systemu rzeczywistego.
- **bezpośrednie,** polegają na sprawdzaniu przyjętych rozwiązań bezpośrednio w badanym systemie. W przypadku nowowprowadzanych systemów telekomunikacyjnych metody bezpośrednie stosuje się budując systemy (sieci) pilotowe. Badania systemu można realizować dwoma metodami, badając: rzeczywisty system funkcjonujący w realnych warunkach oraz model systemu przy zdefiniowanych warunkach oddziaływania otoczenia na jego funkcjonowanie. Cechy poszczególnych metod wymieniono w tabeli 10.1.

Badania systemów wykonywane są głównie na ich modelach. W większości przypadków rozpatrywanie wszystkich szczegółów systemu i wpływu otoczenia nie jest konieczne. Przy opracowaniu modelu celowo pomija się wiele charakterystyk rozpatrywanego systemu i wpływu otoczenia wybierając tylko te, które są istotne z punktu widzenia określonego zadania. Uzyskany tą drogą model reprezentuje, więc pewien wyidealizowany wariant systemu rzeczywistego.

Pojęcie symulacji można zdefiniować następująco:

> ***Symulacja jest techniką numeryczną służącą do realizacji eksperymentów na pewnej klasie modeli matematycznych, które opisują za pomocą programu komputerowego zachowanie się rzeczywistego sytemu (obiektu badanego) w ciągu długiego przedziału czasu.***

Można stwierdzić, że:

- symulacja jest procesem konstruowania w chronologicznym porządku opisów stanów tworzących historię stanów;
- symulacja nie jest czynnością lecz jest procesem.

Włączenie zmiennych losowych do modelu pozwala na wykorzystanie eksperymentu do wnioskowania na temat zachowania się badanego systemu dla różnych rozkładów prawdopodobieństw tych zmiennych losowych.

W każdej chwili system znajduje się w konkretnym stanie. Stan systemu w dowolnej chwili określony jest przez stany jego wszystkich elementów. Jeżeli w różnych chwilach elementy systemu znajdują się w identycznych stanach, to stan systemu w obu chwilach jest dokładnie taki sam. Stan systemu jest określony przez opis stanu, a w sensie czasu jest to punkt. Aby scharakteryzować opis zachowania się systemu w określonym przedziale czasu należy więc podać opisy wszystkich stanów

systemu, w których w interesującym nas przedziale czasu przebywał system. Innymi słowy trzeba skonstruować "historię stanów" lub inaczej chronologicznie uporządkowany opis stanów, w których znajdował się system w analizowanym przedziale czasu. Należy zauważyć, że prowadzącego badania systemu najczęściej interesują stany systemu opisujące określone właściwości systemu, dlatego też mówimy o „częściowej" lub niekompletnej historii stanów.

Tabela 10.1 Cechy metod badawczych systemów i sieci telekomunikacyjnych

Cechy		Metoda		
		Analityczna	**Symulacyjna**	**Bezpośrednia**
Zalety		- duża zgodność uzyskiwanych wyników - niski koszt badań (papier i ołówek) - możliwość badania systemu w fazie prac teoretycznych	- duża zgodność uzyskiwanych wyników - modyfikowalność modelu, możliwość wielokrotnego jego użycia - możliwość badania systemu w fazie prac teoretycznych - możliwość badania żywotności systemu - duża elastyczność modelu (możliwość opisu różnych złożonych zjawisk) - „nieograniczony" zakres badań (w funkcji czasu, parametrów systemu itp)	- badanie na „żywym organizmie" lub wersji pilotowej - weryfikacja teorii z praktyką
Wady		- skomplikowany opis matematyczny otoczenia oddziałującego na system - konieczność posiadania dużej wiedzy teoretycznej (technicznej i matematycznej) - wysoka czasochłonność opisu modelu - ograniczony zakres badań jednokrotność wykorzystania modelu - opis pojedynczych cech systemu - przyjmowanie uproszczeń systemu	- konieczność posiadania drogiego oprogramowania symulacyjnego - konieczność posiadania dużej wiedzy teoretycznej (technicznej i matematycznej) - wysoka czasochłonność opisu pierwszego modelu - przyjmowanie uproszczeń systemu	- badanie na „żywym organizmie" - wysokie koszty badań - konieczność modyfikacji systemu w celu zbierania danych dot. jego pracy - na ogół brak możliwości badań żywotności systemu - dotyczy jedynie systemów istniejących, już zbudowanych - na ogół brak możliwości modyfikacji badanego systemu - ograniczony zakres badań

10.2 Modelowanie obiektu badań symulacyjnych

Model badanego systemu (sieci). Przy uwzględnieniu relacji, jakie zachodzą między badanym systemem a jego otoczeniem, ogólny model badanego systemu może być przedstawiany w następującej postaci:

$$S = \langle H, X, W, \Phi \rangle$$

gdzie: H - model struktury systemu,
X - model otoczenia,
W - model funkcjonowania,
Φ - relacje zachodzące pomiędzy elementami modelu.

Zatem dla odwzorowania systemu niezbędna jest znajomość struktury i parametrów elementów systemu (model elementów systemu), struktury i charakterystyk zewnętrznych czynników wymuszających (model otoczenia), algorytm funkcjonowania systemu (model funkcjonowania) oraz współzależności zachodzących pomiędzy jego elementami.

Model elementów systemu można przedstawić w postaci:

$$H = \langle G, F_q, F_u \rangle$$

gdzie*:*

- **G** to graf (zbiór wierzchołków i łuków grafu) opisujący liczbę i sposób połączeń między sobą węzłów telekomunikacyjnych:

  $$\mathrm{G} = \langle \mathrm{Q}, \mathrm{U}, \mathrm{P} \rangle$$

  $\mathrm{Q} = \left\{ q_n ; n = \overline{1, N} \right\}$ - zbiór wierzchołków grafu, które będziemy utożsamiali z węzłami telekomunikacyjnymi,

  $\mathrm{U} = \left\{ u_m ; m = \overline{1, M} \right\}$ - zbiór gałęzi grafu, które będziemy utożsamiali z liniami telekomunikacyjnymi lub wiązkami łączy międzywęzłowych,

  $\mathrm{P} \subset \mathrm{Q} \times \mathrm{U} \times \mathrm{Q}$ - relacja trójczłonowa wiążąca ze sobą zbiór wierzchołków ze zbiorem gałęzi.
- $\mathbf{F_q}$ - zbiór funkcji określonych na zbiorze wierzchołków grafu,
- $\mathbf{F_u}$ - zbiór funkcji określonych na zbiorze gałęzi grafu.

W badanych modelach ocenowych systemu do parametrów charakteryzujących gałęzie można zaliczyć: wartości przepływności gałęzi, długości gałęzi, natężenie ruchu w gałęzi oraz intensywność uszkodzeń i napraw. Do parametrów charakteryzujących węzły telekomunikacyjne badanych modeli można zaliczyć: wydajność, intensywność uszkodzeń węzłów, intensywność napraw, intensywność narażeń i typy odporności.

Model otoczenia to zbiór czynników zewnętrznych oddziałujących na funkcjonowanie systemu oraz ulegający zmianom pod wpływem działania systemu telekomunikacyjnego.

Model funkcjonowania systemu. Zadania realizowane przez system telekomunikacyjny są zazwyczaj rozpatrywane pod kątem przekazywania wiadomości pod różną postacią. Są one realizowane w systemie przy wykorzystaniu określonych reguł sterowania strumieni wiadomości, uwzględniających stan poszczególnych jego elementów, jak również zakres, stopień pilności i aktualności potrzeb informacyjnych abonentów. Funkcjonowanie systemu telekomunikacyjnego jest związane z realizacją określonych działań, w ramach przyjętych reguł sterowania, obejmujących badanie i zmianę stanu elementów systemu oraz analizę parametrów strumienia wiadomości.

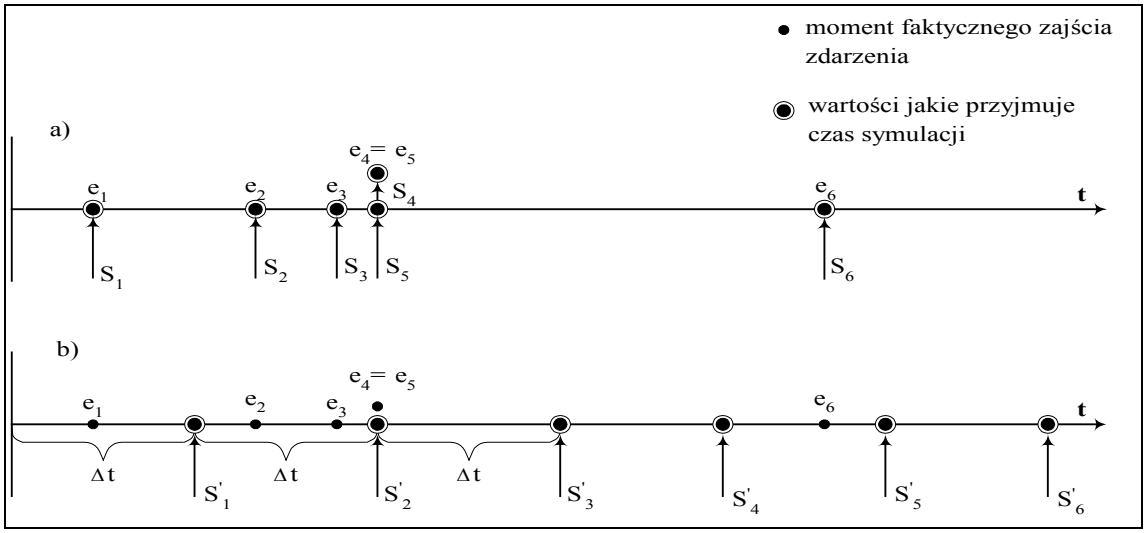
Relacje zachodzące między elementami modelu określają mechanizm zmiany stanów systemu telekomunikacyjnego. Jest to zbiór funkcji, które wyznaczają relacje zachodzące między elementami modelu systemu, modelem funkcjonowania oraz modelem otoczenia.

W symulacji systemów dyskretnych mogą być wykorzystane dwie metody sterowania upływu czasu (rysunek 10.1):

- metoda kolejnych zdarzeń;
- metoda stałego kroku.

W metodzie kolejnych zdarzeń czas systemowy każdorazowo ustawiany jest na chwilę, w której wystąpi kolejne zdarzenie. Każde zdarzenie jest rozpatrywane przez program sterujący w chwili jego wygenerowania a w zasadzie w chwili czasu, która została przypisana zdarzeniu jako czas jego zajścia.

W metodzie stałego kroku natomiast zdarzenia są rozpatrywane w chwilach czasu określonych przez wielokrotność przedziału Δt niezależnie od wyznaczonego momentu jego zajścia. Wynika z tego, że wszystkie zdarzenia, które pojawiły się w przedziale czasu Δt_i będą rozpatrywane w czasie określonym przez koniec tego przedziału.



Rysunek 10.1 Upływ czasu systemowego metodą: a) kolejnych zdarzeń, b) metodą stałego kroku

10.3 Pakiet symulacyjny COMNET III

Program COMNET III kalifornijskiej firmy CACI Products Company jest narzędziem programowym przeznaczonym do analizy i projektowania sieci telekomunikacyjnych. Lista referencyjna podawana przez firmę CACI jest długa, wśród wielu użytkowników wymieniane są przedsiębiorstwa: British Telecom, AT&T, Bell Northern Research, Hewlett Packard, Alcatel Siemens - Nixdorf, Newbridge Networks.

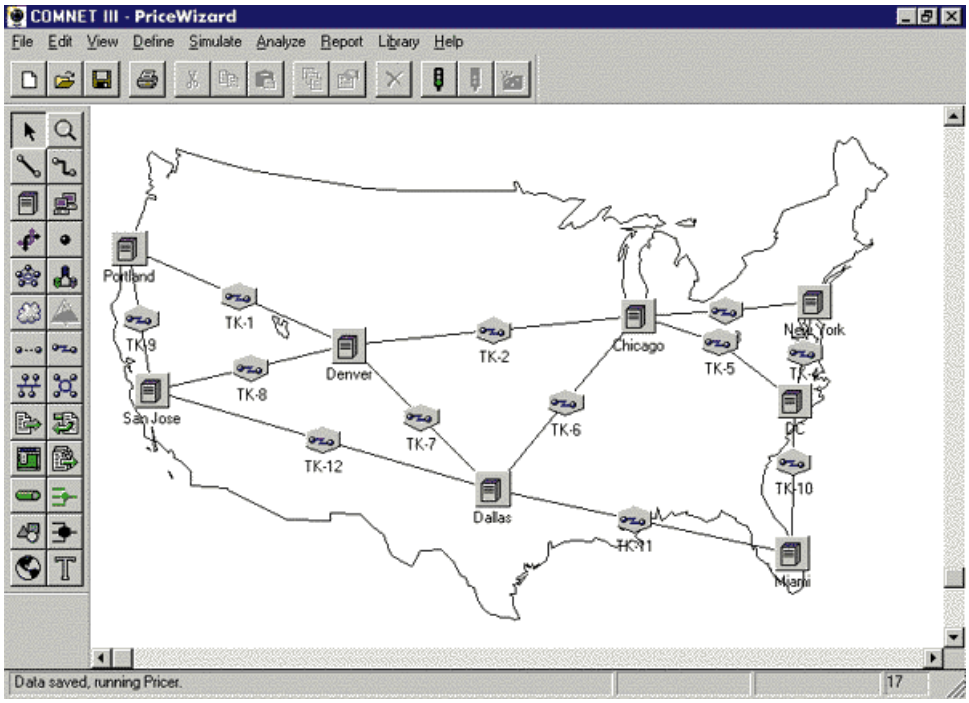
COMNET III pozwala modelować:

- sieci rozległe, metropolitalne, lokalne - model może składać się z wszystkich typów sieci jednocześnie;
- sieci z komutacją łączy, kanałów, pakietów, wiadomości;
- ruch zorientowany na połączenia jak i bezpołączeniowy;
- sieci cyfrowe z integracją usług - N- i B-ISDN (ATM).

Na rysunku 10.2 przedstawiono przykładowy wygląd okna programu Comnet III.

Zbudowane modele mogą być traktowane jako komponenty biblioteczne przeznaczone do budowy nowych modeli. Może on być przydatny w każdej firmie telekomunikacyjnej oferującej swe usługi w zakresie budowy i eksploatacji sieci.

Jak wcześniej wspomniano, COMNET przeznaczony jest dla inżynierów, projektantów systemów telekomunikacyjnych. Narzędzie to pozwala im na szybką i rzetelną ocenę parametrów projektowanych sieci telekomunikacyjnych. Analiza wyników symulacyjnych modelu daje odpowiedź, w jakim stopniu przyszła sieć spełniać będzie określone wcześniej wymagania.



Rysunek 10.2 Okno pakietu COMNET III

Opierając się na opisie sieci, algorytmach sterowania i algorytmach pracy, COMNET przeprowadza symulację zdarzeń zachodzących w modelu sieci i pozwala na analizę jej parametrów. Z doświadczeń uzyskanych tą metodą wynika, że otrzymane charakterystyki (przy założeniu poprawności i adekwatności modelu opisującego projektowaną sieć) są zgodne z danymi empirycznymi z pracy sieci rzeczywistej.

Jest to aplikacja, która nie wymaga od użytkownika znajomości programowania. Opis modelu sieci jest tworzony w prosty sposób, przy wykorzystaniu wygodnego interfejsu graficznego z użytkownikiem, który znacznie przyspiesza tworzenie modelu. COMNET również zapewnia wygodną i zrozumiałą prezentację wyników symulacji.

Większość parametrów rzeczywistych systemów telekomunikacyjnych znajduje swoje odzwierciedlenie w modelu. Opisy urządzeń, czy też operacji sieciowych (występujących w realnie funkcjonujących sieciach), posiadają w modelu swoje odpowiedniki. Podobieństwo to jest tak dalekie, że producenci oprogramowania stworzyli bibliotekę modeli produkowanych urządzeń sieciowych.

COMNET III posiada dużą bibliotekę modeli obiektów. Dotyczy to parametrów węzłów i linii, klas marszrutyzacji, protokołu transportowego dla wiadomości, tablic opłat dla algorytmów marszrutyzacji, rozkładów i tablice rozkładów prawdopodobieństwa. Jeśli nowy obiekt jest tworzony może on być dołączony do programu jako obiekt biblioteczny. Zasoby biblioteczne są czytane automatycznie podczas uruchamiania pakietu COMNET. Zasoby mogą być edytowane, dodawane mogą być nowe obiekty. W bibliotece znajduje się wiele obiektów zdefiniowanych przez CACI.

Opierając się na opisie sieci, algorytmach sterowania i algorytmach pracy, COMNET przeprowadza symulację zdarzeń zachodzących w modelu sieci i pozwala na analizę jej parametrów. Z doświadczeń uzyskanych tą metodą wynika, że otrzymane charakterystyki (przy założeniu poprawności i adekwatności modelu opisującego projektowaną sieć) są zgodne z danymi empirycznymi z pracy sieci rzeczywistej.

Jest to aplikacja, która nie wymaga od użytkownika znajomości programowania. Opis modelu sieci jest tworzony w prosty sposób, przy wykorzystaniu wygodnego interfejsu graficznego z użytkownikiem, który znacznie przyspiesza tworzenie modelu. COMNET zapewnia wygodną i zrozumiałą prezentację wyników symulacji.

Większość parametrów rzeczywistych systemów telekomunikacyjnych znajduje swe odzwierciedlenie w modelu. Opisy urządzeń, czy też operacji sieciowych (występujących w realnie funkcjonujących sieciach), posiadają w modelu swoje odpowiedniki. Podobieństwo to jest tak dalekie, że producenci oprogramowania stworzyli bibliotekę modeli produkowanych urządzeń sieciowych.

Z wykorzystaniem COMNET III można prowadzić następujące badania systemów i sieci telekomunikacyjnych:

- Analiza szczytów obciążenia sieci. Sieć telekomunikacyjna jest obiektem, który cechuje zróżnicowane natężenie ruchu w poszczególnych okresach dnia, tygodnia, miesiąca, roku. Jeśli sieć może wykonywać swe funkcje na określonym wysokim poziomie natężenia ruchu, to może także pracować z mniejszym obciążeniem. COMNET III pozwala modelować okresy, w których poziom obciążenia jest wysoki. Pozwala to na określenie najsłabszych punktów sieci.
- Optymalizacja sieci na podstawie projektu. COMNET III może być wykorzystany na etapie projektowania do oszacowania czy przyszła sieć obsłuży odpowiedni poziom ruchu, czy też nie.
- Elastyczność i niezawodność. Często bardzo ważne jest czy projekt przyszłej sieci oferuje racjonalny poziom żywotności w zależności od różnych scenariuszy uszkodzeń. Węzły i linie w COMNET III mogą ulegać uszkodzeniom i być naprawiane w procesie symulacji. Testowanie tego typu sytuacji, które nie są możliwe do sprawdzenia w systemach rzeczywistych, można realizować w COMNET.
- Wprowadzanie nowych użytkowników/aplikacji. Nowi użytkownicy czy też nowe aplikacje wprowadzają do sieci więcej informacji. Pożyteczne jest przewidzieć ich wpływ na możliwość potencjalnej niewydolności sieci i rozwiązać ten problem przed jego wystąpieniem.
- Doskonalenie sieci. W wielu sieciach ruch rośnie z roku na rok. Rezultatem jest stopniowane pogorszenie się funkcjonalności sieci. Za pomocą COMNET można badać różne opcje unowocześniania sieci w funkcji kosztów.
- Szacowanie możliwości świadczenia poziomu jakości usług. COMNET III może być wykorzystany do analizy dostarczanego poziomu usług, który może być osiągnięty podczas negocjacji, można określić za jego pomocą obszary potencjalnych problemów. Ogólnie przyjętą praktyką jest negocjowanie kontraktu poziomu usług pomiędzy użytkownikiem sieci a jej właścicielem, nawet jeśli są oni częścią tej samej organizacji.

Z wykorzystaniem COMNET III nie można prowadzić następujących badań systemów i sieci telekomunikacyjnych:

- Bezpośrednich kalkulacji cenowych. COMNET nie posiada elementów taryfikacji i kosztu elementów.
- Automatycznej optymalizacji. COMNET nie wskazuje optymalnego projektu sieci, nie określa też jak ma się zmieniać projekt sieci, by zwiększyć jej wydajność. Podejście jest takie, że użytkownik określa model sieci, zaś COMNET przeprowadza symulację i określa jej wydajność. Użytkownik decyduje jak zmienić

sieć, wprowadza zmiany, uruchamia proces symulacji modelu i sprawdza czy parametry sieci uległy polepszeniu.

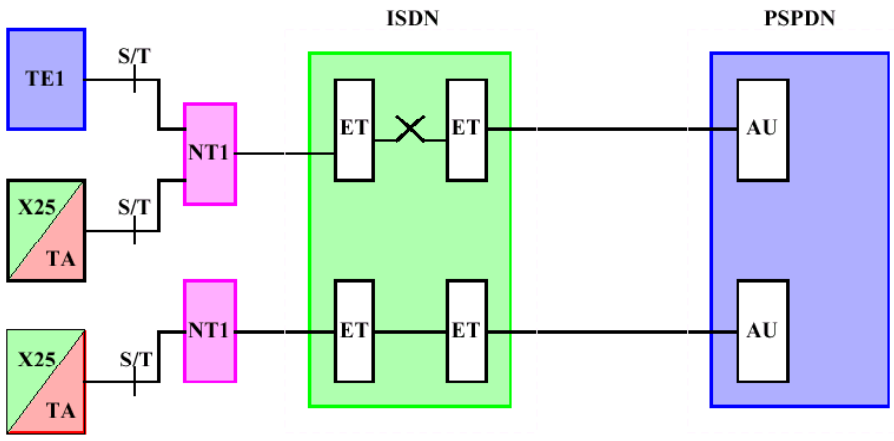
- Dynamicznej zmiany topologii. Koncepcją COMNET nie jest rozpatrywanie położenia geograficznego sieci, czy też przemieszczania zasobów sieci. Możliwości łączeniowe węzłów są modelowane, zaś odległości jedynie z punktu widzenia wprowadzanych opóźnień propagacyjnych. COMNET III jest generalnie używany do modelowania sieci nieruchomych niż ruchomych, np. systemów telefonii komórkowej, sieci satelitarnych czy też mobilnych systemów radiowych. Można powiedzieć, że COMNET III może być wykorzystywany do badania sieci, które są sieciami podkładowymi obsługujących takie systemy.
- Rozpatrywania rodzaju medium fizycznego. COMNET nie zapewnia modelowania pierwszej warstwy modelu dla systemów otwartych. Medium fizyczne jest modelowane w kontekście szybkości bitowej, opóźnienia propagacji, błędów bitów, ramek, pakietów.

11 Załącznik - materiały dodatkowe do wykładów

11.1 X.25 w ISDN

Realizacja komutacji pakietów X.25 w sieci ISDN wg X.31A

Obsługa komutacji pakietów realizowana w PSPDN



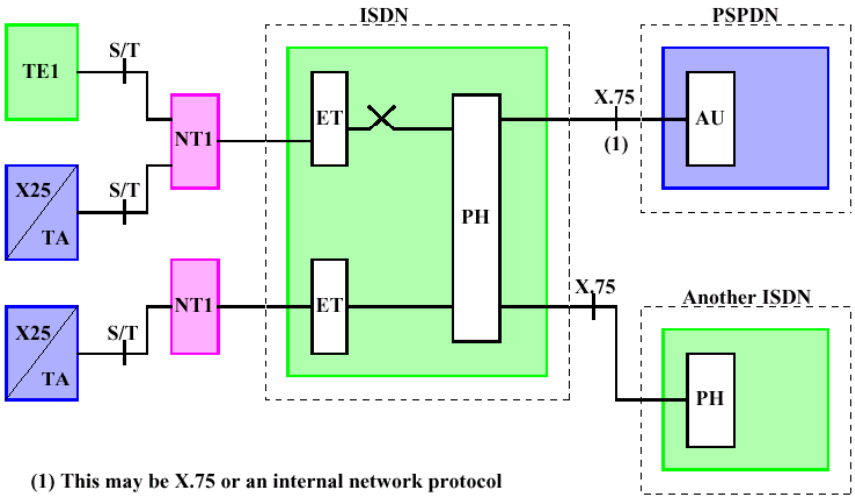
TA – Terminal Adapter **TE – Terminal Equipment**

AU – Adaptation Unit **PSPDN – Public Switch Packet Data Network**

Teleinformatyka

Realizacja komutacji pakietów w sieci ISDN - X.31B

Obsługa komutacji pakietów realizowana w ISDN



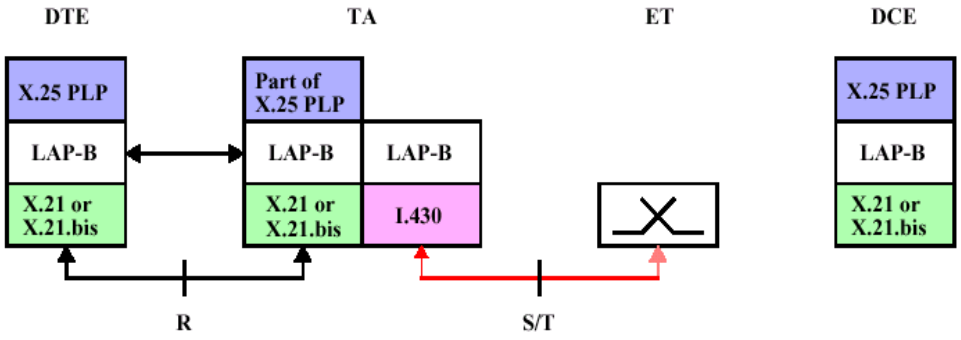
(1) This may be X.75 or an internal network protocol

TA – Terminal Adapter **TE – Terminal Equipment**

AU – Adaptation Unit **PSPDN – Public Switch Packet Data Network**

Teleinformatyka

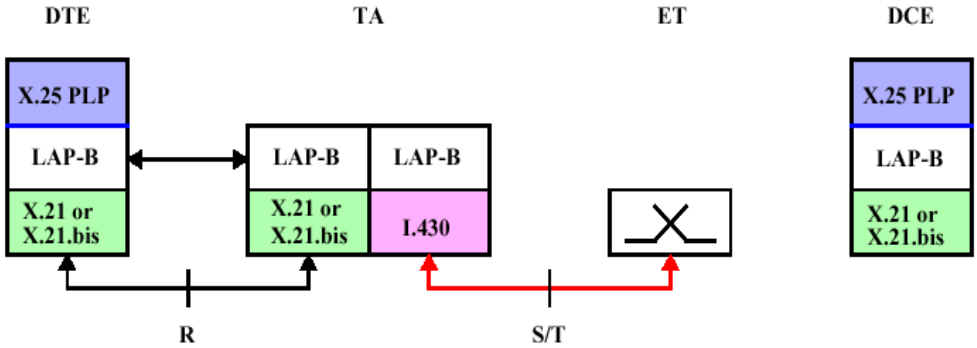
Realizacja komutacji pakietów w sieci ISDN z udziałem warstwy sieciowej



- Nietransparentna realizacja komutacji pakietów z wykorzystaniem mechanizmu Q.931 w warstwie sieci w kanale sygnalizacyjnym D
- Wykorzystana procedura zestawiania kanału wirtualnego

Teleinformatyka

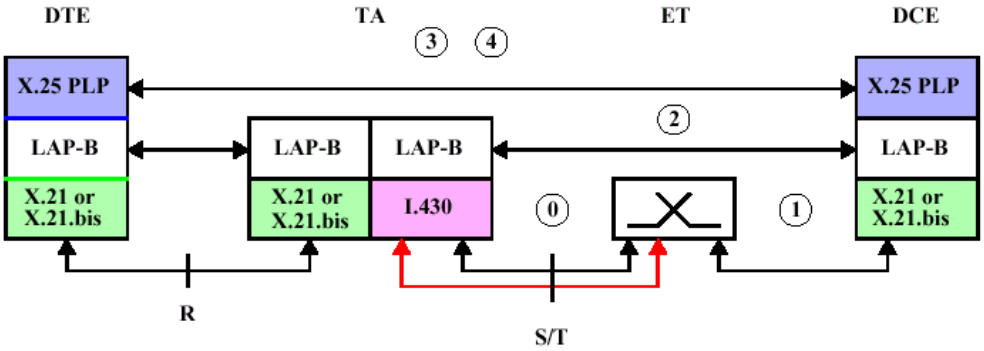
Realizacja komutacji pakietów w sieci ISDN bez udziału warstwy sieciowej



- Transparentna realizacja komutacji pakietów z wykorzystaniem mechanizmu Q.931 w warstwie sieci w kanale sygnalizacyjnym D
- Jedynie wykorzystywane procedury w warstwie łącza i fizycznej
- Metoda stosowana w dostępie dedykowanym

Teleinformatyka

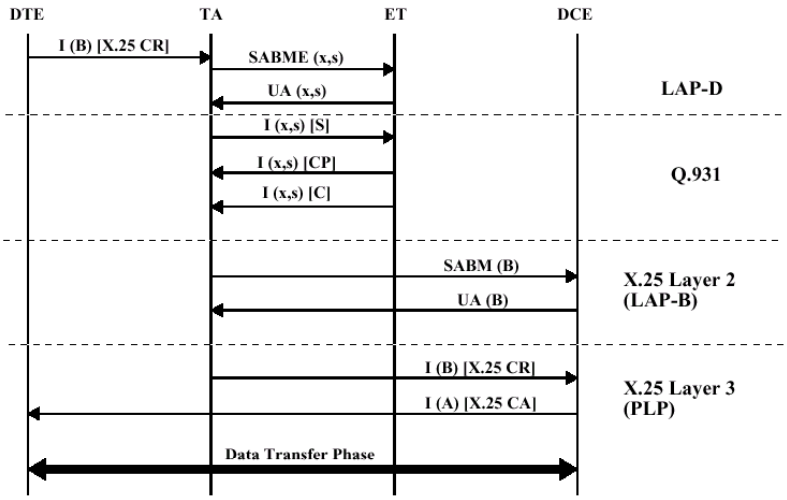
Aktywność warstw w fazie zestawiania połączenia pakietowego z PSPDN



0. Zestawianie kanału B z wykorzystaniem procedur Q.931 po odebraniu ramki informacyjnej z DTE (adres B) zawierającej pakiet Call Request
1. Zestawienie kanału B poprzez sieć ISDN do DCE w PSPDN
2. Zestawienie połączenia w warstwie LAP-B pomiędzy DTE i PSPDN (DCE)
3. Synchronizacja warstwy 3 pomiędzy DTE i DCE
4. Realizacja procesu transferu wiadomości

Teleinformatyka

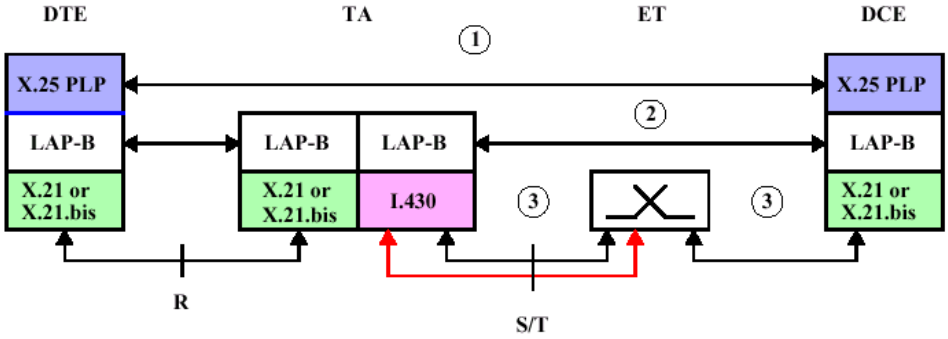
Aktywność warstw w fazie zestawiania połączenia pakietowego z PSPDN cd..



(x,s)	Ramka adresowana do SAPI 0	[S]	Wiadomość Setup message
[X.25 CR]	Call Request	[CP]	Wiadomość Call Proceeding
[X.25 CR]	Call Accepted	[C]	Wiadomość Connect

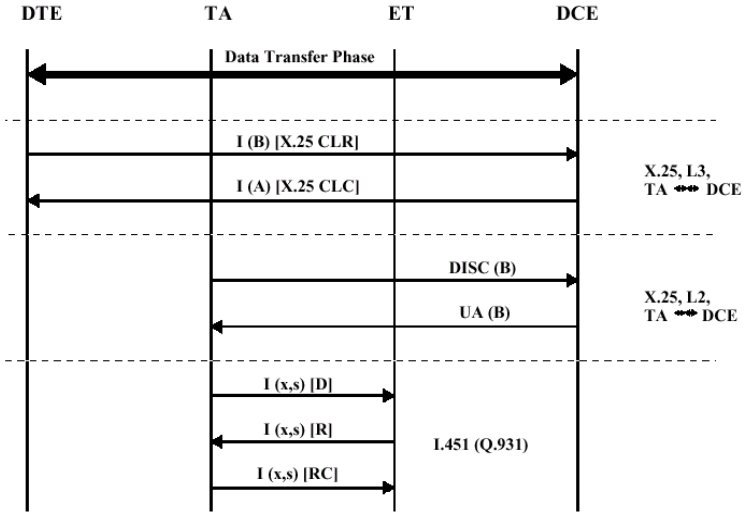
Teleinformatyka

Aktywność warstw w fazie zwalniania połączenia pakietowego



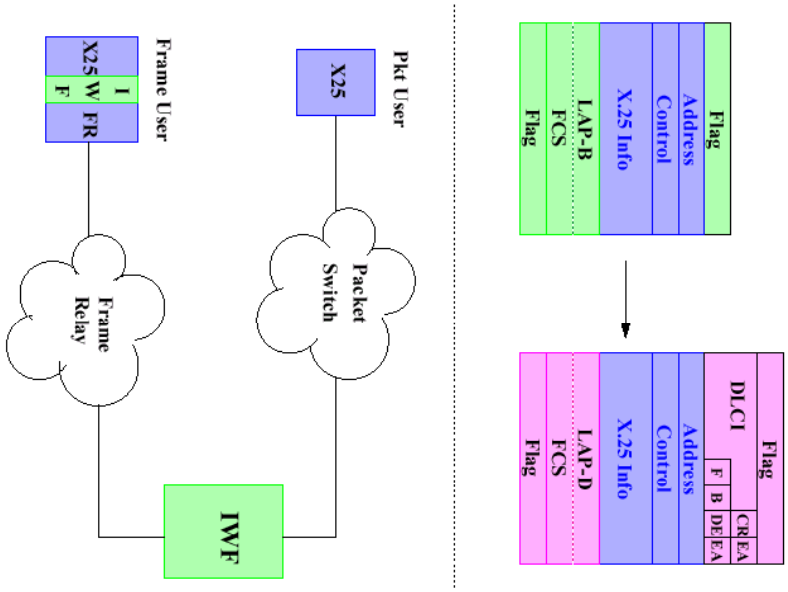
1. Połączenie w warstwie pakietowej jest zerowane przez centralę po wysłaniu pakietów Clear Request i Clear Confirmation
2. Zerowanie warstwy łącza LAP-B po wymianie ramek DISC i UA
3. Zwolnienie kanału B przez centralę po wymianie wiadomości Release i Release Complete

Aktywność warstw w fazie zwalniania połączenia pakietowego



(x,s)	Ramka adresowana do SAPI 0	[D]	Wiadomość Disconnect
[X.25 CLR]	Clear Request	[CP]	Wiadomość Release
[X.25 CLC]	Clear Confirmation	[C]	Wiadomość Release Complete

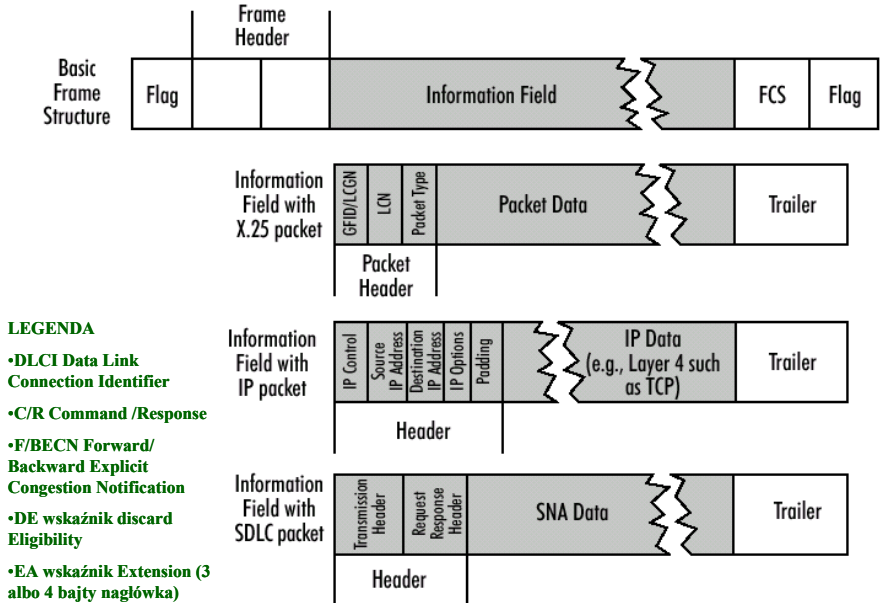
X.25 na Frame Relay



Teleinformatyka

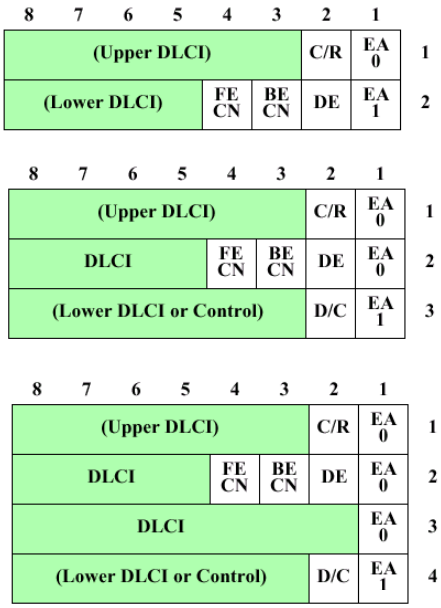
11.2 Frame Relay

Struktura ramki i nagłówka ramki Frame Relay



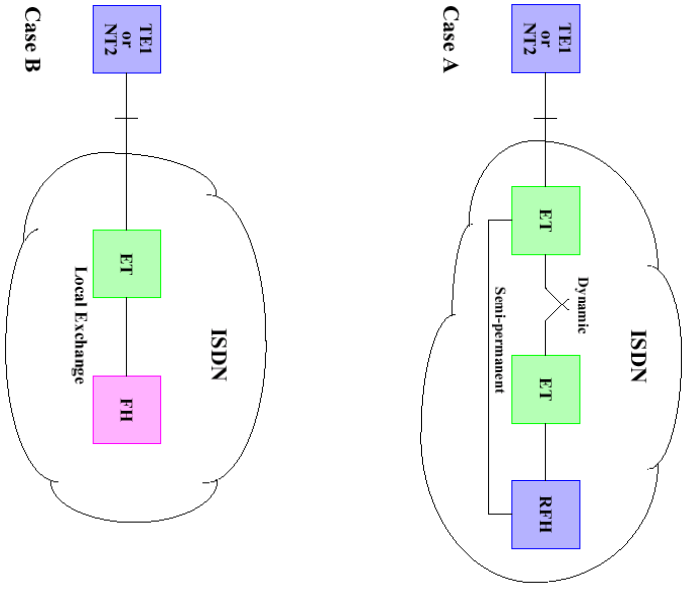
Teleinformatyka

Typy nagłówka ramki Frame Relay



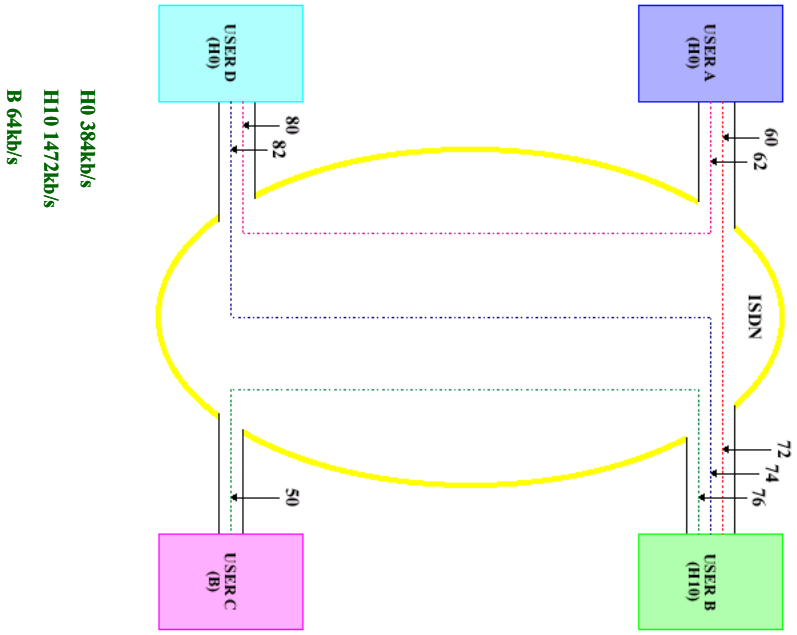
Teleinformatyka

Metody operacji obsługi ramek Frame Relay (Q.933)



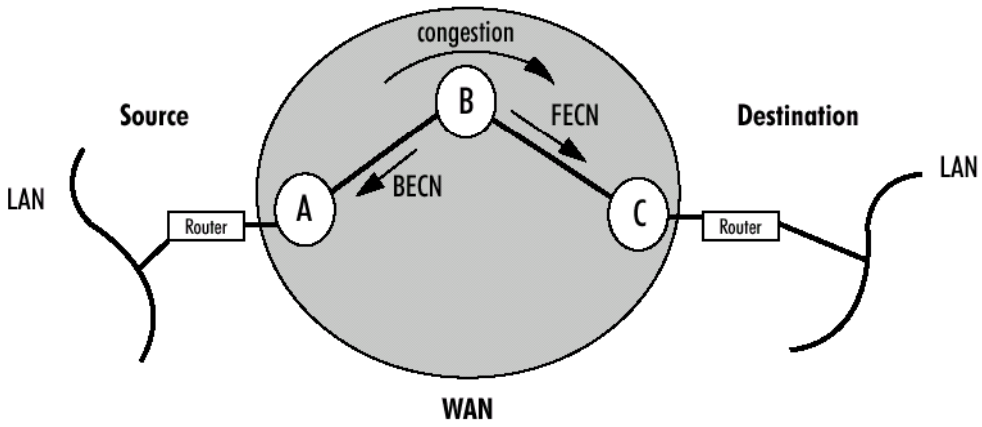
Teleinformatyka

Współpraca abonentów Frame Relay



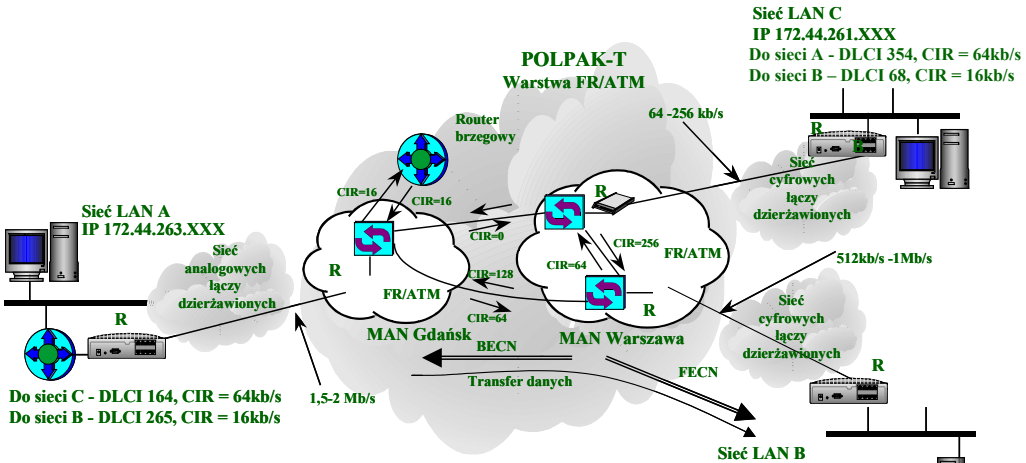
Teleinformatyka

Obsługa Frame Relay w warunkach przeciążenia



Teleinformatyka

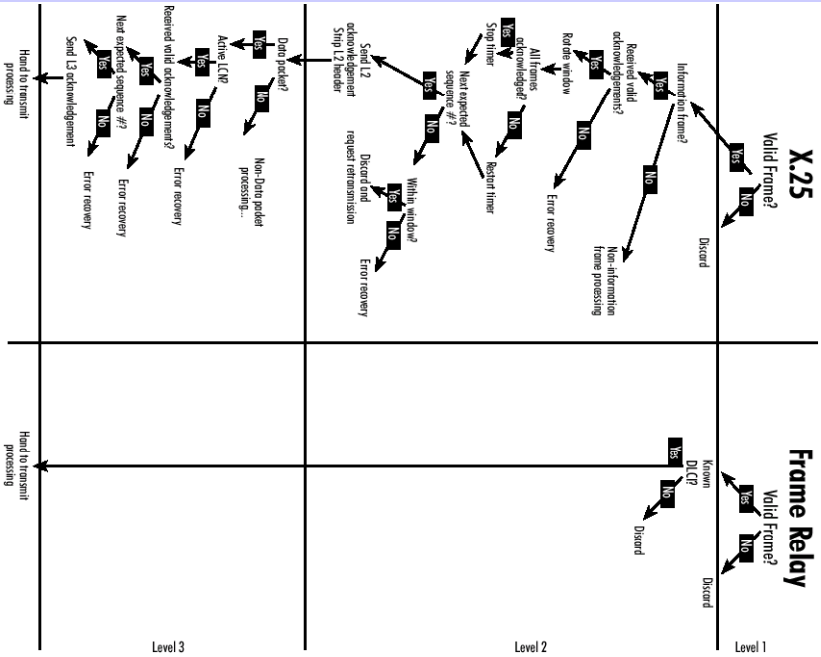
Stałe kanały wirtualne PVC w sieci Frame Relay



Legenda:
R – router
DLCI (Data Link Connection Identifier) – numer kanału logicznego
FECN (Forward Explicit Congestion Notification) – informacja o przeciążeniu nadawana w przód
BECN (Backward Explicit Congestion Notification) - informacja o przeciążeniu nadawana w tył
DE - Discart Eligibility

Teleinformatyka

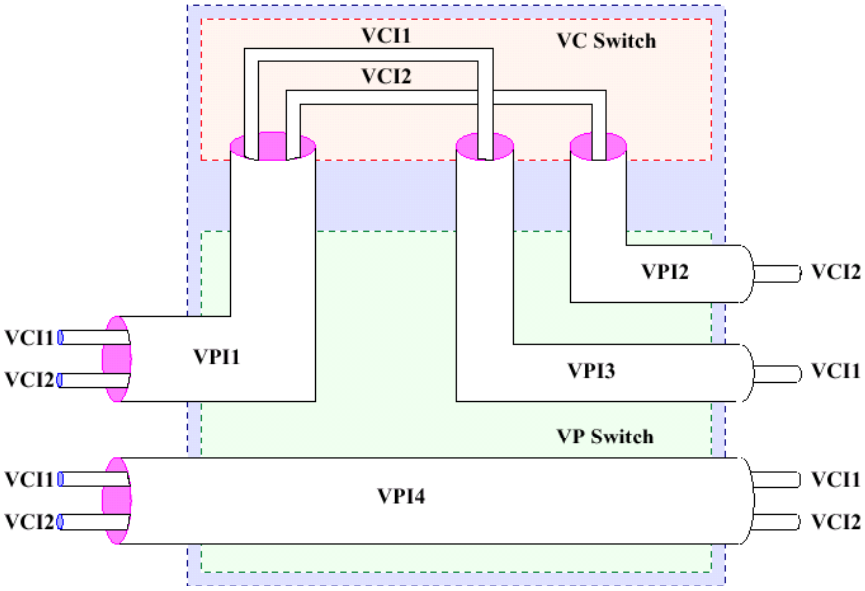
Porównanie uproszczonych modeli przetwarzania wiadomości X.25 i F/R



Teleinformatyka

11.3 ATM

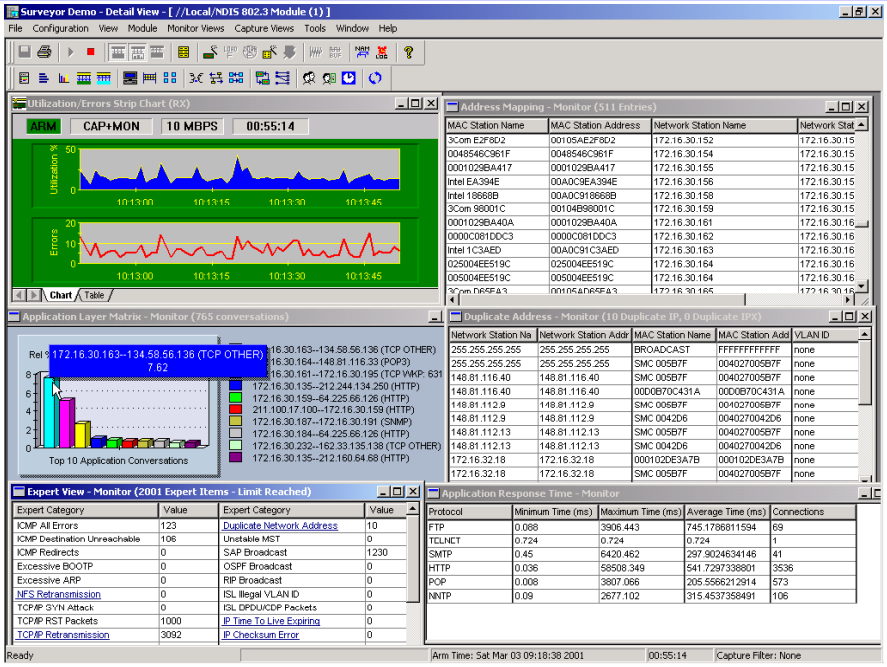
Kanały i ścieżki wirtualne w protokole ATM



Teleinformatyka

11.4 Bezpieczeństwo w sieciach teleinformatycznych

Analiza przepływu informacji w sieci z wykorzystaniem aplikacji Surveyor



Bezpieczeństwo w sieciach teleinformatycznych

Literatura:

1. W. Brzeziński „Sieci LAN", Politechnika Warszawskia
2. A. Wolisz "Podstawy lokalnych Sieci Komputerowych"
3. F. Halsall "Data Communications Computer Networks and Open Systems"
4. W. Stallings "Networking Standarts A Guide to OSI, ISDN, LAN, and MAN Standards"
5. National Semiconductor, IsoEthernet, 1995.