

1. Łącza analogowe i cyfrowe

Łącza służą do przenoszenia sygnału, często nazywane są również mediami fizycznymi. Łącza można podzielić pod względem rodzaju przenoszonego sygnału na:

- Łącza cyfrowe (ang. *digital*), w których transmitowane są sygnały dyskretne (zależnie od poziomu napięcia sygnałom tym przypisuje się wartość logiczną "0" lub "1").
- Łącza analogowe (ang. *analog*), w których transmitowane są sygnały ciągłe (najczęściej o częstotliwościach z zakresu 300-3300 Hz).

Ważną cechą łącz jest liczba strumieni danych, które tymi łączami mogą być przesyłane. Część łączy umożliwia tylko transmisję w jednym kierunku (ang. *half-duplex*) - sygnały nadawane są naprzemiennie, raz z jednej, raz z drugiej strony łącza. Drugą grupę stanowią łącza, znacznie częściej dziś stosowane, pozwalające na równoczesną dwukierunkową transmisję danych (ang. *full-duplex*).

Wielkościami charakterystycznymi dla łącz są: zasięg i prędkość przesyłu danych. Parametry te zebrane zostały w poniższej tabeli:

Kabel	Typowe szerokości pasma i odległości
Skretka kategorii 5	10-100 Mb/s, 100 m
Koncentryczny 50 ohm (cienki)	10-100 Mb/s, 200 m
Koncentryczny 75 ohm (gruby)	10-100 Mb/s, 500 m
Światłowód wielomodowy	100 Mb/s, 2 km
Światłowód jednomodowy	100-2400 Mb/s, 40 km

Tabela: Zestawienie najważniejszych parametrów popularnych mediów fizycznych

Pamiętajmy jednak, że nie wszystkich łączy można używać wymiennie. Przed wyborem łącza powinniśmy zastanowić się jaki rodzaj techniki będziemy wykorzystywać do transmisji danych.

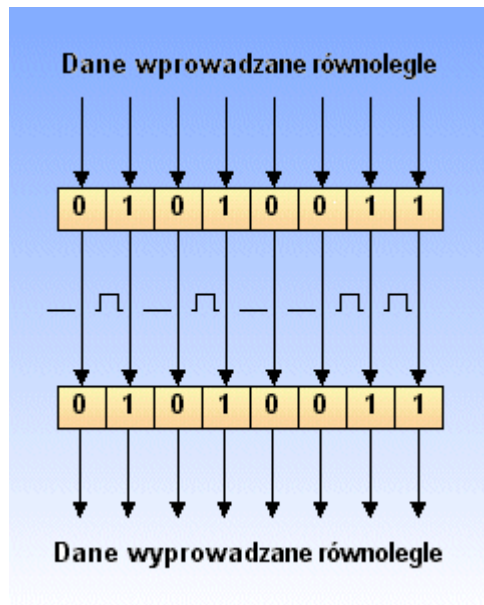
[NASTĘPNA](#)

2. Rodzaje transmisji sygnału i RS-232

(2.1) Transmisja szeregowa i równoległa

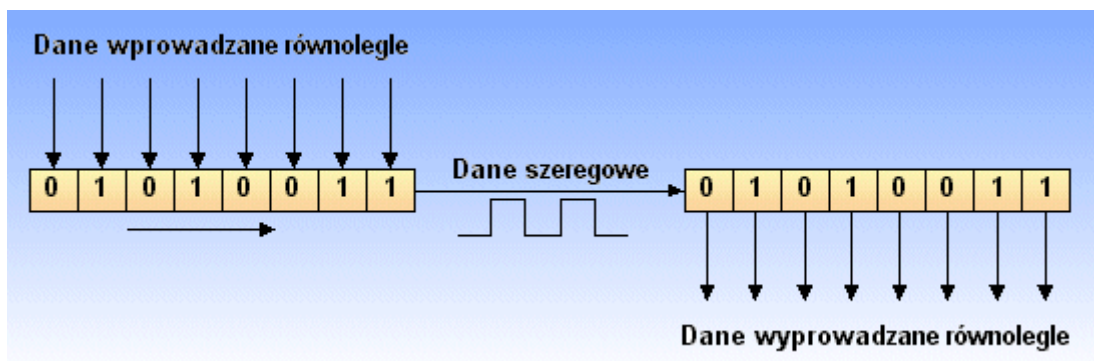
Transmisja sygnału może przebiegać w różnoraki sposób. Najbardziej podstawowym z podziałów, jest podział transmisji sygnału na równoległą i szeregową.

Transmisja równoległa polega na przesyłaniu wszystkich bít słowa danych jednocześnie (patrz rysunek 8.1.). Za względu na fakt, że sprzęt komputerowy, w naturalny sposób wspiera taki sposób wprowadzania/wyprowadzania danych, transmisja równoległa jest bardzo popularna. Ponadto, dzięki zrównolegleniu przesyłu danych, uzyskujemy znaczny przyrost prędkości przesyłu. Udogodnienia te wiążą się jednak z faktem konieczności stosowania łączy dziewięcioprzewodowego, nieodzownego przy tego rodzaju transmisji.



Rysunek 8.1. Transmisja równoległa

Transmisja szeregowa polega na sekwencyjnym przesyłaniu danych bit po bicie. Należy zaznaczyć, że informacja wprowadzana jest do rejestru przesuwającego styku szeregowego, który bit po bicie wysyła ją na wyjście układu [1].



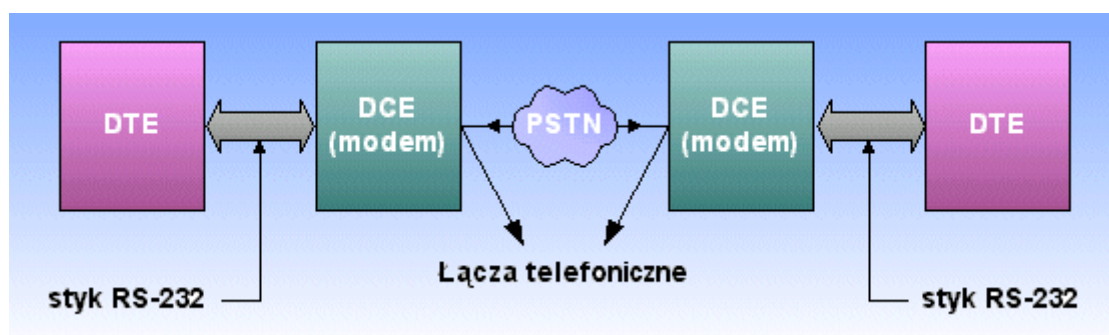
Rysunek 8.2. Transmisja szeregowa

Zaletą tego rodzaju transmisji jest możliwość przesyłu danych na dużo większą odległość niż w

przypadku transmisji równoległej, a przy tym konieczne są jedynie dwa przewody do transmisji (jednostronnej) sygnału. Wadą tej techniki na pewno jest fakt, że transmisja odbywa się znacznie wolniej oraz to, że styki szeregowo wymagają większej złożoności obwodów wewnętrznych.

(2.2) Standard RS-232

Standard RS-232 opisuje sposób połączenia urządzeń DTE (ang. *Data Terminal Equipment*) tj. urządzeń końcowych danych (np. komputer) oraz urządzeń DCE (ang. *Data Circuit-terminating Equipment*), czyli urządzeń komunikacji danych (np. modem). Standard podaje nazwy styków złącza oraz przypisane im sygnały a także specyfikację elektryczną obwodów wewnętrznych.



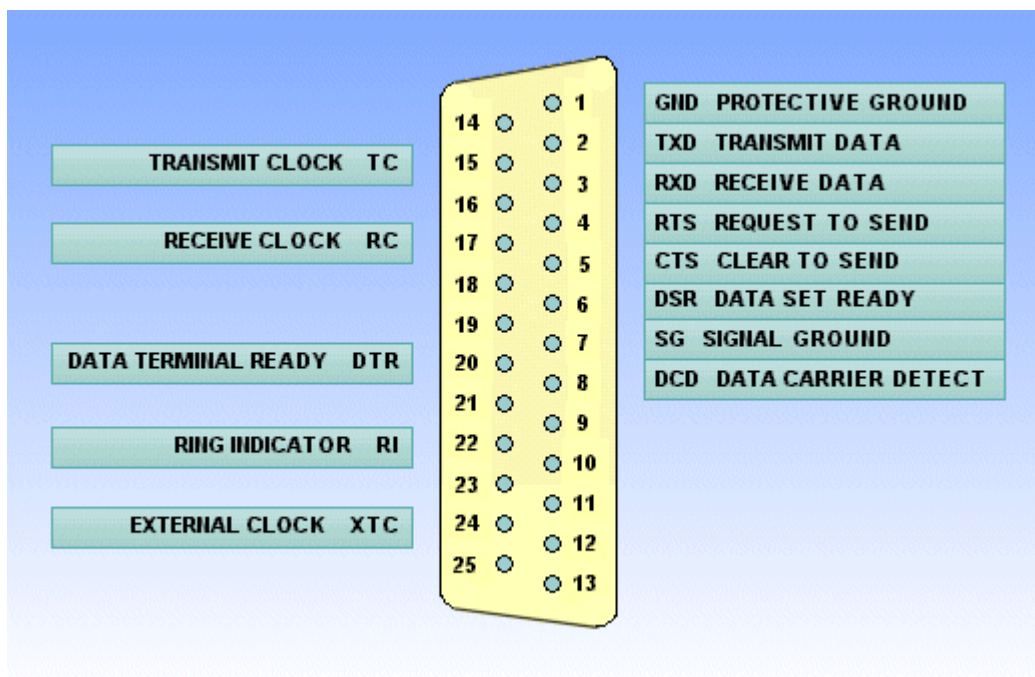
Rysunek 8.3. Wykorzystanie łącza RS-232 [1]

RS-232 jest stykiem przeznaczonym do szeregowej transmisji danych. Specyfikacja opisuje 25 styków. Najbardziej popularna wersja tego standardu, RS-232-C pozwala na transfer na odległość nie przekraczającą 15 m z szybkością maksymalną 20 kbit/s.

Specyfikacja napięcia definiuje "1" logiczną jako napięcie -3V do -15V, zaś "0" to napięcie +3V do +5V. Poziom napięcia wyjściowego natomiast może przyjmować wartości -12V, -10V, 10V, +10V, zaś napięcie na dowolnym styku nie może być większe niż +25V i mniejsze niż -25V. Należy zaznaczyć przy tym, że zwarcie dwóch styków RS-232 nie powoduje jego uszkodzenia [1].

(2.3) Wymiana danych przez RS-232

Złącze RS-232 zawiera 25 styków, które należą do czterech głównych grup związanych z funkcjami jakie pełnią. Rysunek 8.4. przedstawia złącze RS-232 w urządzeniu DTE wraz z oznaczeniami ważniejszych wyprowadzeń.



Rysunek 8.4. Styk RS-232 urządzenia DTE [1]

Obwody opisane przez standard RS-232 dzielimy następująco [1]:

1. **Obwody podstawy czasu** niezbędne podczas transmisji synchronicznej.

XTC	<i>eXtemal Clock signal</i>	podstawa czasu dla sygnałów nadawanych przez urządzenie DTE
RC	<i>Receive Clock signal</i>	elementarna podstawa czasu, która jest odtwarzana w DCE
TC	<i>Transmit Clock signal</i>	podstawa czasu dla sygnałów nadawanych przez urządzenie DTE

2. **Obwody przekazywania danych** używane do transmisji szeregowej danych.

TXD	<i>Transmit Data</i>	DTE nadaje dane do DCE
RXD	<i>Receive Data</i>	DTE odbiera dane od DCE

3. **Obwody uziemienia.**

SG	<i>Signal Ground</i>	uziemienie sygnałowe
GND	<i>protective GrouND</i>	uziemienie ochronne

Styk SG ustala wspólny zerowy potencjał DTE oraz DCE. Styk GND zmniejsza liczbę błędów wywołanych przez zakłócenia.

4. Obwód sterownia (najważniejsze styki).

DTR	<i>Data Terminal Ready</i>	gotowość urządzenia DTE
DSR	<i>Data Set Ready</i>	gotowość urządzenia DCE
RTS	<i>Request To Send</i>	żądanie nadawania
CTS	<i>Clear To Send</i>	gotowość do nadawania
DCD	<i>Data Carrier Detect</i>	poziom sygnału odbieranego
RI	<i>Ring Indicator</i>	wskaźnik wywołania

Sygnały przesyłane w tych obwodach są przeznaczone głównie do ustawiania połączenia oraz nadzorowania półdupleksowego sposobu pracy łącza.

Łącze odpowiedzialne za transmisję może pracować w trzech trybach: duplexowym - FDX, półduplexowym - HDX, a także simpleksowym - SX. Łącze w trybie duplexowym może stosować system automatycznej retransmisji ARQ (ang. *Automatic Repeat reQuest*), który zapewnia powtórny transmisję danych po wykryciu błędu transmisji [1]. W łączu simpleksowym możliwe jest stosowanie korekcji błędów FEC (ang. *Forward Error Correction*), która polega na dodaniu pewnych danych do przekazu, w celu zapewnienia korekcji błędów po stronie odbierającej.

[NASTĘPNA](#)

3. Zasada działania modemu i łącza modemowe

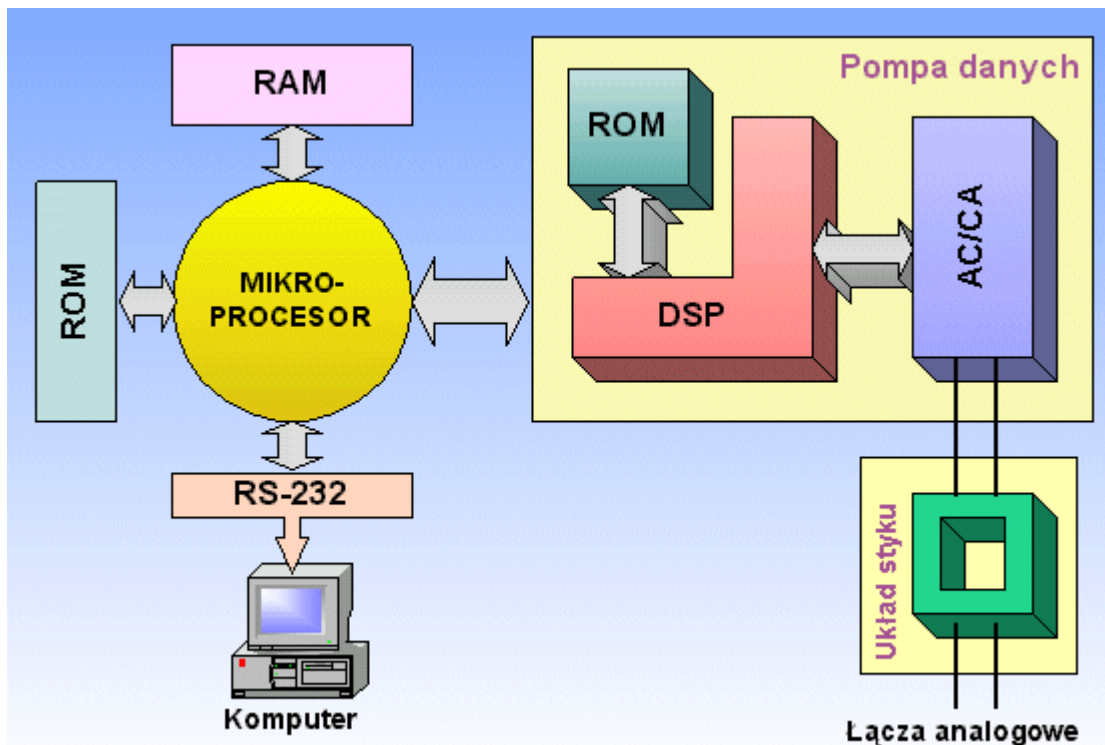
Modem (*MODulator-DEModulator*) to urządzenie, którego zadaniem jest konwersja sygnału cyfrowego na analogowy oraz sygnału analogowego w cyfrowy. Modemy służą do zestawiania połączeń z wykorzystaniem komutowanych łączy telefonicznych, w których sygnał (głos) ma postać analogową. Dlatego też, aby umożliwić transmisję sygnału cyfrowego z naszego komputera, poprzez łącza telefoniczne, do komputera odległego, konieczna jest zamiana sygnału cyfrowego w analogowy. Proces taki odbywa się poprzez modulację sygnału cyfrowego. Aby po stronie odbiorcy możliwy był odbiór analogowego sygnału przesyłanego łączyami telekomunikacyjnymi, konieczny jest proces zamiany sygnału analogowego na cyfrowy. Osiąga się to poprzez demodulację sygnału analogowego.

Modemy, które komunikują się za pośrednictwem łączy telefonicznych muszą stosować takie same techniki komunikacyjne. Do najważniejszych z nich należą standardy CITT (ang. *Consultative Committee for International Telegraph and Telephone*). Drugi popularny standard to jest MNP (*Microcom Networking Protocol*).

Modem podłączany jest do komputera zwykle za pomocą łącza RS-232 i może być wykonany jako karta rozszerzająca (modem wewnętrzny), jak i osobne urządzenie montowane na zewnątrz komputera.

(3.1) Budowa modemu

Poniżej przedstawimy rysunek poglądowy, który pozwala poznać relacje pomiędzy poszczególnymi składowymi modemu.



Rysunek 8.5. Wewnętrzna budowa modemu

Elementy przedstawione na rysunku mają określone funkcje. Oto one:

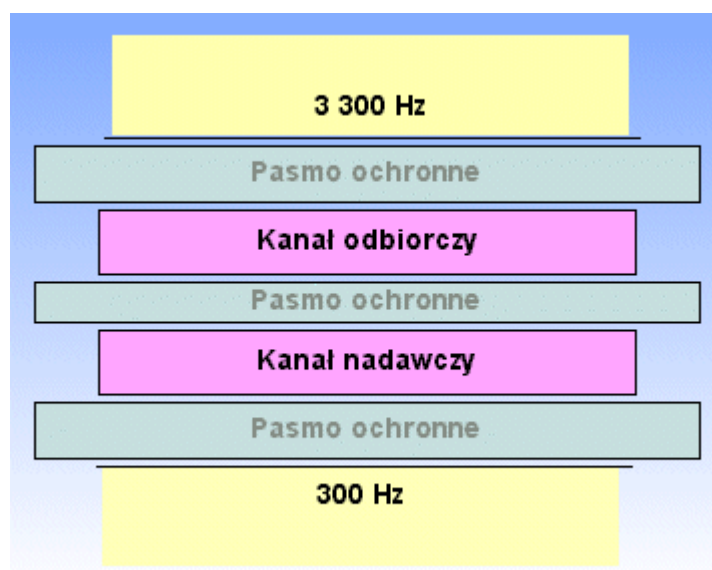
- o **Pompa danych** (ang. *Data Pomp*). Zadaniem tego właśnie układu jest modulacja/demodulacja

sygnałów. W środku pompy danych znajduje się procesor sygnałowy DSP, który posiada zawarte w pamięci ROM określone procedury modulacji (np. zgodnie ze standardem CCITT), również przetworniki AC/CA, dzięki którym możliwa jest konwersja cyfra/analog i analog/cyfra. Ponadto zadaniem układu jest eliminacja różnego rodzaju zakłóceń.

- o **Mikroprocesor** steruje pracą całego układu. Mikroprocesor posługuje się wewnętrznym językiem AT, za pomocą rozkazów którego możliwa jest komunikacja pomiędzy komputerem i modemem, wybieranie numeru telefonu adresata, kompresja danych i kodowanie zabezpieczające. Program sterujący mikroprocesorem znajduje się w pamięci ROM, procesor dysponuje również pamięcią podręczną RAM.
- o **RS-232**, czyli układ transmisji szeregowej, zajmuje się transmisją danych pomiędzy komputerem a modemem.
- o **Łącze** odpowiedzialne jest za pulsacyjne wybieranie numeru oraz izolację galwaniczną linii telefonicznej od modemu.

(3.2) Łącza modemowe

Pasma przenoszenia dla linii telekomunikacyjnych wynosi około 3000 Hz. Jest ono wystarczające do transmisji głosu. Podczas transmisji danych musimy wziąć pod uwagę fakt, że ze względu na różnice w jakości połączeń telefonicznych nie jest możliwe, aby całe pasmo było przeznaczone do transmisji danych. Dlatego też stosowane są pasma ochronne, których rola jest prosta: oddzielić częstotliwość nadawczą od odbiorczej (dla trybu duplex). Zadaniem pasma ochronnego jest zabezpieczenie sygnału przed zakłóceniami.



Rysunek 8.6. Łącza telefoniczne

Istnieją dwa rodzaje łączy umożliwiających komunikację modemową:

1. Łącze komutowane - połączenie odbywa się poprzez dzielenie łącza. Połączenie jest zestawiane pomiędzy dwoma adresatami, zakończenie rozmowy powoduje likwidację łącza.
2. Łącze dzierżawione - różni się tym od łącza komutowanego, że nie występuje nawiązywanie i rozłączanie połączenia, połączenie zestawiane jest na stałe.

[NASTĘPNA](#)

4. Protokoły sieciowe

Pojęcie protokołów sieciowych odnosi się głównie do tych protokołów, które są związane z warstwami modelu OSI. Protokoły umożliwiają korzystanie z adresów, dzięki którym dostarczenie dowolnie dużej porcji danych na nieokreśloną odległość nie stanowi właściwie problemu.

Nazwa warstwy modelu referencyjnego OSI	Numer warstwy OSI
Aplikacji	7
Prezentacji	6
Sesji	5
Transportu	4
Sieci	3
Łącza danych	2
Fizyczna	1

Tabela: Model referencyjny OSI

Warto wiedzieć, że protokoły warstwy 3 wykorzystują pewną strukturę danych - pakiet. Ponadto dostarczają mechanizmów do wysyłania pakietów. Pamiętajmy, że warstwa 3 nie gwarantuje poprawności kolejności przesyłu danych oraz dostarczenia pakietu do adresata. Te zadania realizuje warstwa 4 modelu referencyjnego OSI. Protokoły tej warstwy przekazują dane z warstw wyższych i umieszczają je w segmentach, które są przekazywane warstwie 3.

(4.1) NetBEUI

NetBEUI (ang. *NetBIOS Extended User Interface*), czyli rozszerzony sieciowy interfejs użytkownika NetBIOS (podstawowy system sieciowych operacji wejścia-wyjścia) został stworzony przez IBM i pojawił się na rynku komputerowym w 1985 roku.

NetBEUI został zaprojektowany do użytku tylko w sieciach lokalnych LAN. Jego zadaniem jest zapewnienie komunikacji pomiędzy dwoma komputerami, niezawodności dostarczenia i odpowiedniej kolejności pakietów. Opiera się więc na 3 i 4 warstwie modelu referencyjnego OSI. Dzięki takiej specyfikacji nie możliwe jest trasowanie pakietów do sieci zewnętrznych. Wiadomości trasowane do sieci zewnętrznych muszą być opakowane z użyciem protokołów np. TCP/IP czy IPX. Należy wspomnieć również, że NetBEUI dość znacznie obciąża sieć ze względu na rozgłoszeniowy system komunikacji (np. aby znaleźć wymagany komputer, protokół wysyła zapytanie do wszystkich komputerów w sieci LAN). Niewątpliwymi zaletami protokołu jest są minimalne wymagania dotyczące pamięci oraz dobra ochrona przed błędami transmisji.

NetBEUI, niezależnie od wersji, jest integralną częścią systemów operacyjnych firmy Microsoft.

(4.2) IPX/SPX

IPX/SPX (ang. *Internet Packet Exchange / Sequenced packed echange*) to zestaw protokołów międzysieciowej wymiany pakietów / sekwencyjnej wymiany pakietów firmy Novell. Konstrukcja IPX/SPX oparta jest o popularny niegdyś system firmy Xerox - XNS. Na rynku ta rodzina protokołów zaistniała na początku lat 80-tch jako integralna część systemu sieciowego Novell Netware [2].

Protokół IPX jest bezpołączeniowym protokołem datagramowym, który nie zapewnia dostarczenia pakietu do adresata. Protokół IPX wymaga współpracy z protokołem SPX, który z kolei zapewnia uporządkowanie pakietów w odpowiedniej kolejności wysłania, zapewnia gwarancję dostarczenia pakietów oraz pozostałe usługi warstwy 4 modelu referencyjnego OSI. Poniżej przedstawiamy stos protokołów IPX/SPX w odniesieniu do modelu OSI.

Nazwa warstwy modelu referencyjnego OSI	Numer warstwy OSI	Opis równoważnej warstwy IPX/SPX			
Aplikacji	7	R I P	S A P	N C P	N L S P
Prezentacji	6				
Sesji	5				
Transportu	4				SPX
Sieci	3	Miedzysieciowa wymiana pakietów			
Łącza danych	2	Interfejs otwartego łącza danych			
Fizyczna	1	Dostęp do nośnika			

Rysunek 8.7. Model referencyjny OSI a IPX/SPX [2]

Stos protokołów IPX/SPX obejmuje cztery podstawowe warstwy:

- warstwę aplikacji
- warstwę Internetu
- warstwę łącza danych
- warstwę dostępu do nośnika

Nazwy warstw odpowiadają funkcjom, jakie pełni każda z nich. Poniżej opisane zostały warstwy rodziny protokołów IPX/SPX.

Warstwa aplikacji

Warstwa aplikacji IPX/SPX odpowiada trzem warstwom modelu referencyjnego OSI: aplikacji, prezentacji i sesji. Jednak część protokołów warstwy aplikacji jest dostępna także w niższych warstwach OSI.

Rdzeń warstwy aplikacji stanowi protokół NCP (ang. *NetWare Core Protocol*) [2], który można zestawiać z protokołem IPX oraz SPX. Protokół rdzenia zapewnia współdzielenie plików, poczty elektronicznej, dostęp do katalogów oraz możliwość drukowania.

Kolejnym protokołem jest protokół informacyjny trasowania RIP (ang. *Routing Information Protocol*). Działanie protokołu jest bardzo proste. Do wyboru drogi wykorzystywane są dwie metryki: kwanty (ang. *ticks*) oraz skoki (ang. *hops*). Kwant to okres czasu, zaś skok jest przejściem przez router. Podstawą wyboru trasy są kwanty, zaś w przypadku równych wartości kwantów - porównywane są skoki. Wadą tego protokołu jest duży poziom narzutu sieciowego - aktualizacja

tabeli RIP jest dokonywana co 60 sekund.

Protokół SAP (ang. *Service Advertisement Protocol*) natomiast wykorzystywany jest przez serwery do automatycznej okresowej wysyłki informacji o dostępnych usługach. Wysyłki te, oprócz wspomnianych informacji, określają serwer, tzn. jego typ, nazwę i status operacyjny, opisują również numer sieci i gniazda. Zgłoszenia SAP mogą być również wykorzystywane przez klientów, którzy potrzebują określonej usługi. Takie zgłoszenie jest rozgłaszane w całym segmencie sieci, a hosty mające możliwość udostępnienia wymaganej usługi odpowiadają wysyłając informację SAP, zawierającą również odległość do danego hosta. Wadą tego protokołu jest wysyłanie informacji o usługach co 60 sekund.

Ostatnim z protokołów warstwy aplikacji, które opiszemy jest protokół obsługi łącza systemu Netware, czyli NLSP (ang. *Netware Link Services Protocol*). NLSP jest następcą protokołów RIP i SAP. Jest to protokół trasowania. Aktualizacja trasy nie dokonuje się jednak okresowo, jak w przypadku wyżej wymienionych starszych protokołów, lecz wyłącznie w przypadku zajścia jakichkolwiek zmian.

Warstwa Internetu

Warstwa Internetu obejmuje warstwę 3 i 4 modelu referencyjnego OSI. W tej warstwie znajdują się dwa główne protokoły rodziny Netware. Są to IPX i SPX. SPX jest protokołem warstwy 4, IPX należy do warstwy 3. Oba protokoły można uznawać za odpowiedników popularnych protokołów TCP i IP. Poniżej krótko scharakteryzujemy oba protokoły.

Protokół SPX to protokół połączeniowy, umożliwiający przesyłanie danych pomiędzy kilkoma klientami, serwerami oraz pomiędzy klientem a serwerem. Protokół daje gwarancję dostarczenia danych pakietów IPX, umożliwia sterowanie strumieniem danych, kontrolę błędów oraz odpowiednią kolejność pakietów. Poniżej przedstawiamy strukturę nagłówka SPX zachowując kolejność pól danych [2]:

- **Sterowanie połączeniem (8-bitów):** cztery 2-bitowe flagi sterują dwukierunkowym przepływem danych.
- **Typ strumienia danych (8 bitów).**
- **Identyfikacja połączenia źródłowego (16-bitów):** identyfikacja procesu, który zainicjował połączenie.
- **Identyfikacja połączenia docelowego (16-bitów):** identyfikacja procesu, który zaaprobował zgłoszenie SPX.
- **Numer sekwencji (16-bitów):** pole zawiera numer wysłanego pakietu, dzięki czemu możliwe jest poukładanie pakietów po stronie odbiorcy we właściwej kolejności.
- **Numer potwierdzenia (16-bitów):** numer wskazuje następny segment.
- **Liczba alokacji (16-bitów):** pole umożliwia śledzenie liczby pakietów wysłanych, a nie odebranych.
- **Dane:** jeden pakiet SPX może zawierać maksymalnie 534 oktety.

Jak już wspomniano protokół IPX należy do warstwy 3 modelu OSI. Jego zadaniem jest bezpołączeniowe dostarczanie datagramów. IPX dołącza do protokołów warstwy wyższej (np. SPX) swój nagłówek i umożliwia wysłanie pakietów poprzez wiele różnych sieci. Nagłówek IPX zawiera

następujące informacje:

- **Suma kontrolna (16-bitów):** pole zapewnia kompatybilność wstecz z protokołem XNS, który pole to wykorzystywał; obecnie ustawiane przez IPX automatycznie na FFFFH.
- **Długość pakietu (16-bitów):** pole zawiera długość datagramu IPX wraz z nagłówkiem i danymi, jest pomocne przy weryfikacji integralności pakietu.
- **Sterowanie transportem (8-bitów):** każdy router, przez który datagram przechodzi, zwiększa to pole o 1, wartość początkowa naturalnie "0".
- **Typ pakietu (8-bitów):** pole identyfikuje typ pakietu zapakowanego do IPX, wartość ta przekazywana jest do wyższej warstwy protokołów.
- **Numer sieci docelowej (32-bity):** pole definiuje numer sieci, w której znajduje się węzeł docelowy (szukany adresat).
- **Węzeł docelowy (48-bitów):** numer węzła docelowego (komputera).
- **Numer gniazda docelowego (16-bitów):** opisuje numer gniazda procesu lub programu odpowiedzialnego za odbiór pakietów.
- **Numer Sieci Źródłowej (32-bity).**
- **Adres Węzła Źródłowego (48-bitów).**
- **Numer Gniazda Źródłowego (16-bitów).**

Z powyższych informacji jednoznacznie wynika, że zastosowanie protokołów SPX, jak i IPX daje duże możliwości funkcjonalne.

Warstwy łącza danych i dostępu do nośnika

Warstwy te odpowiadają dwu najniższym warstwom modelu referencyjnego OSI. Warstwa łącza danych jest kompatybilna ze standardem interfejsu otwartego łącza danych ODI [2]. Warstwa dostępu do nośnika również jest kompatybilna z wszelkimi znormalizowanymi protokołami umożliwiającymi dostęp do nośnika. Dzięki takim rozwiązaniom najniższych warstw rodzina protokołów IPX/SPX znalazła szerokie zastosowanie.

(4.3) AppleTalk

Protokół AppleTalk jest stosowany w sieciach równoprawnych. Odwrotnie niż w sieciach typu klient/serwer, każdy z komputerów może być zarówno serwerem jak i klientem. Stos protokołów AppleTalk składa się z pięciu warstw, które możemy w następujący sposób odnieść do modelu referencyjnego OSI:

Nazwa warstwy modelu referencyjnego OSI	Numer warstwy OSI	Opis równoważnej warstwy AppleTalk
Aplikacji	7	Aplikacji
Prezentacji	6	
Sesji	5	Sesji
Transportu	4	Transportu
Sieci	3	Datagramowa
Łącza danych	2	Dostępu do sieci
Fizyczna	1	

Rysunek 8.8. Model referencyjny OSI a AppleTalk [2]

Jak widać, rodzina AppleTalk jest ściśle oparta na modelu referencyjnym OSI. Poniżej krótko przedstawione zostanie działanie każdej z warstw.

Warstwa aplikacji

Warstwa ta składa się z jednego protokołu. Jest to protokół dostępu do plików w sieci AppleTalk, czyli AFP (ang. *AppleTalk Filing Protocol*). AFP zawiera usługi plików sieciowych, które można dostarczyć aplikacjom, nienależącym do stosu AppleTalk. Aplikacje takie, chcąc nadawać/odbierać muszą wykorzystywać do tego celu protokół AppleTalk.

Warstwa sesji

Warstwa sesji definiuje pięć podstawowych protokołów.

Protokół nr 1 - to protokół strumienia danych sieci AppleTalk - ADSP (ang. *AppleTalk Data Stream Protocol*). ADSP umożliwia zestawienie sesji pomiędzy dwoma odległymi procesami, wykorzystuje do tego adresy gniazd. Protokół ten dostarcza środki do sterowania strumieniem danych, porządkowania kolejności i potwierdzenia dotarcia pakietu do adresata.

Protokół nr 2 gwarantuje dostarczenie danych oraz udostępnia usługi transportowe protokołu ATP (ang. *AppleTalk Transfer Protocol*). Nazywany jest protokołem sesji sieci AppleTalk ASP (ang. *AppleTalk Session Protocol*).

O protokole nr 3 można powiedzieć tylko, że wykorzystywany jest głównie do zarządzania trasą oraz wymianą informacji pomiędzy urządzeniami trasującymi [2]. Protokół ten, nazywany jest protokołem trasowania AppleTalk AURP (ang. *AppleTalk Update-based Routing Protocol*).

Protokół nr 4 to protokół dostępu do drukarki PAP (ang. *Printer Access Protocol*), który został opracowany, aby możliwe było zarządzanie tym urządzeniem. PAP może jednakże być wykorzystywany nie tylko przez drukarki, ale również i inne urządzenia.

Piątym protokołem warstwy sesji jest ZIP (ang. Zone Information Protocol), czyli protokół informacji o strefach. Strefy są grupami urządzeń. Strefy stosuje się w celu łatwiejszego zarządzania tymi urządzeniami.

Warstwa transportu

Warstwa transportowa zapewnia warstwom wyższym możliwość transportu danych. Warstwę transportową tworzą cztery protokoły.

Jako pierwszy przedstawimy najpopularniejszy z protokołów tej warstwy - ATP (ang. *AppleTalk Transport Protocol*). Protokół ten jest gwarantem dostarczenia pakietów. Aby sprawdzić, czy pakiety rzeczywiście dotarły, ATP wykorzystuje pola sekwencji i potwierdzenia, które są odczytywane z nagłówka pakietu.

Drugi z protokołów warstwy transportu to protokół wiązania nazw NBP (ang. *Name Binding Protocol*). NBP współdziała z protokołem warstwy wyższej ZIP. NBP zapewnia rzeczywistą zamianę nazw stref na adresy sieciowe oraz adresy węzłów.

Następny protokół, to protokół echa sieci AppleTalk AEP (ang. *AppleTalk Echo Protocol*). Z jego pomocą można określić dostępność systemu oraz obliczyć czas transmisji a także czas wymagany na potwierdzenie przyjęcia pakietu.

Protokół utrzymania wyboru trasy RTMP (ang. *Routing, Table Maintenance Protocol*) służy do zarządzania tablicami trasowania (obejmuje to dostarczanie routerom tych tablic).

Warstwa datagramowa

Warstwa datagramowa, zgodnie z definicją modelu OSI, umożliwia bezpołączeniowe dostarczanie datagramów. Warstwa ta zajmuje się zestawianiem komunikacji, a także jest odpowiedzialna za dynamiczne adresowanie węzłów sieciowych oraz rozpoznawanie adresów MAC [2].

Główny protokół tej warstwy to protokół dostaw datagramów DDP (ang. *Datagram Delivery Protocol*). Ciekawą cechą protokołu jest zmienny nagłówek, w zależności od adresu adresata. Jeżeli adresat znajduje się w sieci lokalnej, stosowany jest nagłówek standardowy, w przeciwnym wypadku nagłówek rozszerzony o pola: adresu sieci docelowej/źródłowej i licznika skoków. Pola nagłówka DDP przedstawiają się następująco:

- **Liczba skoków** (tylko w nagłówku rozszerzonym). Licznik zwiększany o jeden po każdorazowym dotarciu datagramu do routera.
- **Długość datagramu** - pole używane do sprawdzania, czy datagram nie uległ uszkodzeniu w wyniku transmisji.
- **Suma kontrolna DDP** (opcjonalnie) - stosowana przy korekcji błędów transmisji.
- **Numer gniazda źródłowego** - określa proces, który zrealizował połączenie z naszym komputerem.
- **Numer gniazda docelowego** - określa proces, który odpowiedział na próbę połączenia.
- **Adres źródłowy** (tylko w nagłówku rozszerzonym) - pole zawiera numer sieci i węzeł komputera, który zainicjował połączenie.

- o **Adres docelowy** (tylko w nagłówku rozszerzonym) - pole zawiera numer sieci i węzeł komputera, do którego zrealizowane zostało połączenie.
- o **Typ DDT** - określa jakiego protokołu wyższej warstwy należy użyć dla danego datagramu.
- o **Dane** - dane przesyłane mogą mieć maksymalny rozmiar 586 oktetów.

Drugim protokołem tej warstwy jest AARP (ang. *AppleTalk Address Resolution Protocol*), czyli protokół rozróżniania adresów sieci. AARP jest używany do przekształcania adresów węzłów na adresy fizyczne MAC, można go również użyć w celu określenia adresu węzła konkretnej stacji. Tablica odwzorowywania węzłów AMT przechowuje informacje o adresach węzłów i odpowiadających im adresach MAC.

Warstwa łączy danych

Warstwa łączy danych obejmuje dwie najniższe warstwy modelu referencyjnego OSI. Głównym zadaniem tej warstwy jest włożenie AppleTalk do ramki Ethernet 802.3, która jest klasycznym sposobem przesyłania danych w sieciach rozległych, w tym także w Internecie.

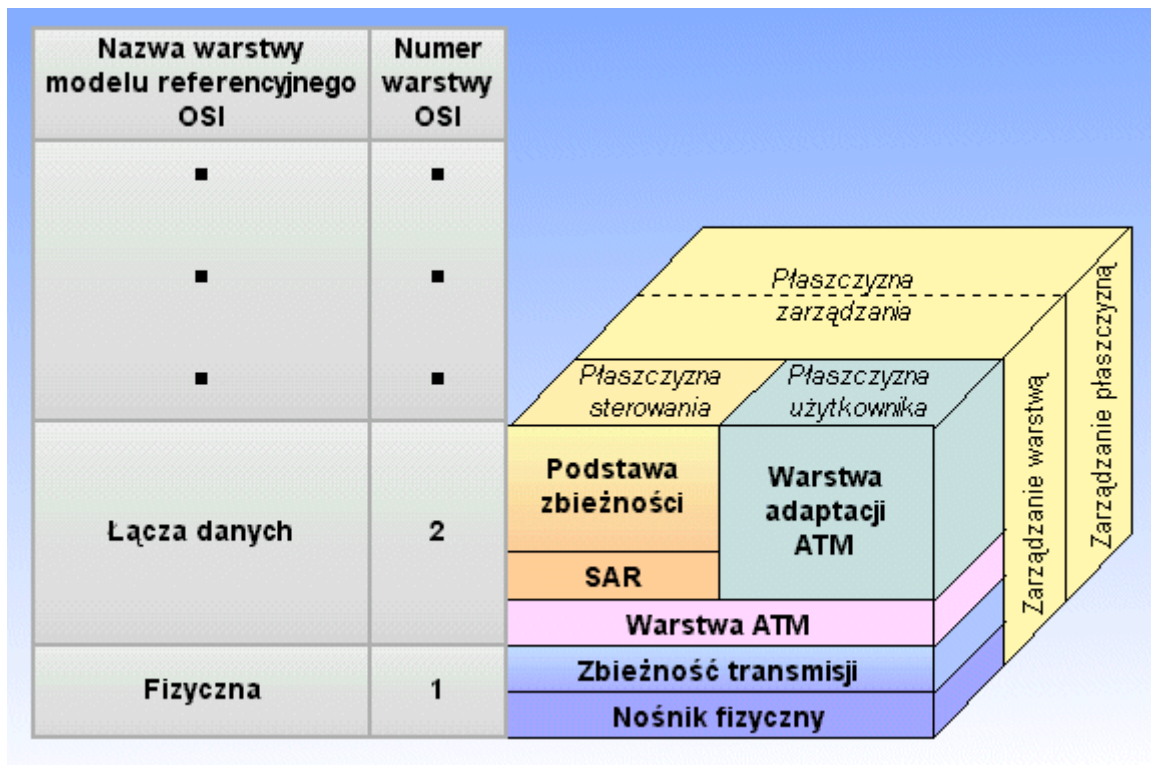
AppleTalk zawiera podwarstwy, stanowiące wsparcie dla FDDI oraz Token Ring. Podwarstwy te nazywają się odpowiednio FDDITalk i TokenTalk. FDDITalk i TokenTalk określa się mianem protokołów dostępu z tego względu, że oferują usługi umożliwiające dostęp do sieci fizycznej.

Jednym z protokołów warstwy łączy danych jest EtherTalk. Protokół ten używa protokołu dostępu szeregowego ELAP (ang. *Ether Talk Link Access Protocol*) w celu pakowania danych i umieszczania ich w ramach Ethernet 802.3 [2]. Inny z protokołów, TokenTalk również korzysta z protokołu o nazwie TLAP (ang. *Token Talk Link Access Protocol*) w celu dostępu do łącza TokenTalk.

Firma Apple oferuje również nowy protokół tej warstwy, nie korzystający ze znanych standardów przesyłania danych w sieciach WAN. Protokół, o którym mowa to LocalTalk. LocalTalk używa protokołu dostępu do łącza LocalTalk o nazwie LLAP (ang. *Local Talk Link Access Protocol*).

(4.4) ATM

Protokół ATM wprowadza zupełnie nowe podejście do koncepcji modelu referencyjnego. Warstwy znane nam do tej pory, w modelu ATM zostały zastąpione przez trójwymiarowe płaszczyzny. Podobnie jak dotychczas, każda z płaszczyzn reprezentuje jakiś pakiet protokołów, odpowiedzialny za określoną część działalności ATM. Rysunek 8.9. przedstawia porównanie modeli referencyjnych OSI i ATM.



Rysunek 8.9. Model referencyjny OSI a ATM

Nietypowość protokołu ATM polega także na ograniczeniu się tylko do dwóch najniższych warstw modelu referencyjnego OSI. Poniżej krótko opiszemy podstawowe warstwy (pamiętając, że warstwa ATM ma trzy wymiary).

Warstwa nośnika fizycznego

Zadaniem warstwy nośnika fizycznego PM (ang. *Physical Medium*) jest współpraca z nośnikiem fizycznym. Zawarte są tu procedury, które umożliwiają wykonywanie zadań takich jak: synchronizacja taktowania transmisji obwodu wirtualnego, wysyłanie/odbieranie bitów. Istnieją różne specyfikacje warstwy nośnika fizycznego dla różnych rodzajów tego nośnika.

Warstwa zbieżności transmisji

Warstwa zbieżności transmisji TC (ang. *Transmission Convergence*) odpowiedzialna jest w sieciach ATM za następujące działania:

1. **Kontrolę błędów sprzętowych HEC** (ang. *Hardware Errors Control*) - suma kontrolna, która jest generowana tylko na podstawie nagłówka (5 oktetów), nie zaś całej komórki (53-oktety).
2. **Określanie komórki** - jest to funkcja, której zadaniem jest zachowanie integralności i granic komórki odbieranej. Umożliwia to wyodrębnienie komórek z odbieranych danych.
3. **Rozdzielenie szybkości transmisji komórek** - polega na zsynchronizowaniu szybkości transmisji komórek w warstwie ATM oraz szybkości transmisji w warstwie nośnika.
4. **Dostosowywanie, generowanie i odzyskiwanie ramki transmisyjnej** - czyli wszelkie procesy związane z zapakowywaniem/odpakowywaniem komórek w/z ramki.

Warstwa ATM

Zadaniem warstwy ATM jest tworzenie połączeń wirtualnych, a następnie przekazywanie za ich pomocą komórek otrzymanych w wyniku działania protokołu AAL. Funkcje, które pełni warstwa ATM, ściśle wiążą się z urządzeniem, w którym warstwa ta się znajduje. Możliwe są dwa warianty:

1. **Stacja końcowa.** Warstwa ATM znajdująca się w stacji końcowej ma możliwość powiadamiania innych stacji o tym, że w jej posiadaniu są dane przeznaczone dla tych właśnie stacji. Ponadto konieczne jest uzgodnienie z innymi "współstacjami" konstrukcji komutowanego obwodu wirtualnego SVC (ang. *Switched Virtual Circuit*). Należy pamiętać, że aby możliwe stało się przyjmowanie danych z warstwy AAL, konieczne jest stworzenie obwodu logicznego. Po tym zabiegu możliwe jest przekształcanie jednostek danych AAL do postaci komórki dodając odpowiednie pola nagłówka.
2. **Przełącznik** (ang. *switch*). Warstwa ATM znajdująca się w przełączniku musi, po odebraniu komórki ze swojego portu, pobrać wartość identyfikatorów VPI oraz VCI (pojęcia te zostaną wyjaśnione później), znajdujących się w nagłówku komórki, a następnie porównać te wartości z tablicą przyporządkowań VPI/VC warstwy ATM. Kolejnym krokiem jest identyfikacja portu docelowego dla przesyłanej komórki. Ponadto warstwa ATM przełącznika gwarantuje buforowanie i porządkowanie komórek, co ma niebagatelne znaczenie, gdy kilka portów wejściowych odwołuje się do jednego poru wyjściowego.

Warstwa adaptacji

Warstwa adaptacji określana jako AAL (ang. *ATM Adaptation Layer*) to zestaw protokołów, który ma trzy wersje AAL 1, AAL 3/4 oraz AAL 5. Każda z warstw jest wykorzystywana do obsługi czterech klas usług ATM: A, B, C oraz D. Zadaniem warstw adaptacji jest umieszczenie danych otrzymanych z warstwy SAR (ang. *Segmentation and Reassembly*) w strukturze o nazwie "jednostka danych protokołu segmentacji i ponownego złożenia" (ang. *SAO-PDU*). Jednostkę taką przekazuje się warstwie ATM, która dokleja do niej 5-oktetowy nagłówek tworząc 53-oktetową komórkę ATM.

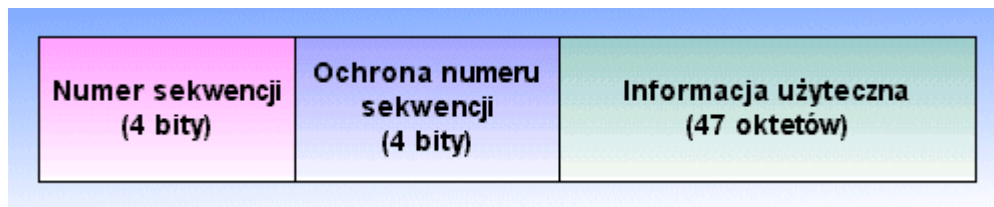
Do warstwy adaptacji wlicza się również **podwarstwę zbieżności**, która jest pośrednikiem pomiędzy protokołami warstwy 3, a protokołami ATM. Umożliwia również zamianę żądań usług AAL, SAR i ATM pochodzących od protokołów warstw wyższych z rodziny TCP/IP, czy chociażby IPX/SPX.

Częścią warstwy adaptacji jest również mechanizm SAR. SAR zamienia strukturę danych otrzymaną z protokołów wyższego rzędu na 48-oktetowe struktury danych ATM [2].

Jak już wspomniano warstwa adaptacji składa się z czterech klas, z których każda określa jakąś usługę sieci ATM. Poniżej przedstawiono usługi każdej z klas:

1. **Usługa klasy A.** Korzysta z warstwy AAL 1 wykorzystując typ transmisji synchronicznej bezpołączeniowej ze stałą szybkością transmisji bitów - CBR (ang. *Constant Bit Rate*). Możliwa jest więc transmisja dźwięku i profesjonalnych filmów wideo. Jednostka SAO-PDU klasy A zawiera dwa dodatkowe 4-bitowe pola:
 - o numer sekwencji SN (ang. *Sequence Number*) - licznik, jest zerowany dla każdej jednostki danych przekształcanej przez SAR;
 - o ochrona numeru sekwencji SNP (ang. *Sequence Number Protection*) - określa cykliczną kontrolę nadmiarową CRC (ang. *Critical Redundancy Check*) i jest obliczana na podstawie pola SN.

Zauważmy, że występowanie obu pól dodatkowych zmniejsza rozmiar ładunku użytecznego komórki AAL 1, co przedstawia rysunek 8.10.:



Rysunek 8.10. Budowa jednostki SAO-PDU

2. **Usługa klasy B.** Różni się tym od usługi klasy A, że nie jest wykorzystywana stała, lecz zmienna szybkość przesyłania bitów VBR (ang. *Variable Bit Rate*). Kolejną różnicą wynika stąd, że usługa klasy B korzystała z warstwy AAL2. Niestety, choć AAL2 rokował duże nadzieje dotyczące przesyłu niektórych sekwencji wideo, nie udało się ukończyć prac nad tą specyfikacją [2]. Dlatego też, usługi tej klasy, nie są dostępne.
3. **Usługa klasy C.** Komunikacja asynchroniczna typu połączeniowego ze zmienną szybkością transmisji bitów. Komunikacja tego typu jest zgodna z komunikacją reprezentowaną przez TCP/IP, IPX/SPX, czy protokoły niższych warstw, np. X.25. Choć wymienione tu protokoły są typu bezpołączeniowego, połączenie w sieci ATM musi zostać ustanowione, później nie ma już ograniczeń związanych z zawartością części użytecznej przesyłanych komórek. Pamiętajmy, że możliwa jest sytuacja, w której protokół sieci ATM opakuje dane protokołów bezpołączeniowych, po czym przesyła je jako pakiety.

Aby sytuacja taka była możliwa, wykorzystywana jest podwarstwa zbieżności, która tworzy jednostkę CS-PDU warstwy AAL 3/4. Później jednostka CS-PDU trafia do warstwy SAR, gdzie jest dzielona na jednostki AAL 3/4 SAO-PDU.

Dla usługi klasy C opracowano również warstwę AAL 5, która zawiera najpopularniejsze części warstwy AAL 3/4. Jest to bardzo wydajna i użyteczna warstwa, której budowa oparta jest na założeniu, że większość obsługiwanych aplikacji wykorzystuje bezpołączeniowe protokoły komunikacyjne. Tak jak w przypadku AAL 3/4 tworzone są (tym razem doskonalsze) jednostki CS-PDU. Następnie AAL 5 CS-PDU jest przekształcana, przez mechanizm SAR, w jednostkę SAO-PDU. Jednostkę AAL 5 SAO-PDU cechuje niezwykła prostota, dzięki czemu jest łatwa w implementacji.

4. **Usługa klasy D.** Bardzo podobna w swej strukturze do usługi klasy C. Klasa D oferuje bezpołączeniowy, asynchroniczny transfer danych i jest wykorzystywana głównie przy przesyłaniu komunikacji sieci typu LAN lub SMDS przez sieć ATM.

(4.5) IrDA

Standard IrDA (ang. *Infrared Data Association*) powstał z inicjatywy trzech firm: HP, Sharp oraz IBM. W 1993 roku standard ten opisuje połączenie typu punkt-punkt (ang. *point-to-point*) w paśmie podczerwieni, charakteryzujące się małym poborem mocy. Dzisiaj możemy korzystać z dwóch wersji protokołu IrDA: 1.0 oraz 1.1. Pierwsza wersja pozwala na transfer rzędu 115 kB/s, zaś druga na szybkość transmisji sięgającą 4Mb/s. Schemat działania standardu IrDA jest następujący. Oba urządzenia (ponieważ każde połączenie jest typu punkt-punkt) nawiązują łączność z prędkością 9600 b/s i sukcesywnie zwiększają transfer, aż do ustalenia prędkości maksymalnej. IrDA pozwala na połączenie urządzeń w odległości nie większej niż 1 m i przy kącie odchylenia nie większym niż 15 stopni, co daje następujący wniosek: urządzenia muszą się "widzieć".

Na standard IrDA składa się kilka protokołów, które wzajemnie korzystają ze swoich usług. **Protokoły obowiązkowe** przesyłu danych w standardzie IrDA to:

- **PHY** (ang. *Physical Signaling Layer*) - zapewnia transfer danych na poziomie 9600 b/s - 4 Mb/s oraz kontrolę poprawności danych CRC (dla transferu poniżej 1.152 CRC-16, powyżej CRC-32). Ponadto oprócz wersji standardowej, istnieje możliwość skorzystania z wersji energooszczędnej, którą charakteryzuje 10-krotnie niższy pobór energii.
- **IrLAP** (ang. *IrDA Link Access Protocol*) - umożliwia uporządkowany transfer danych pomiędzy dwoma urządzeniami.
- **IrLMP** (ang. *IrDA Link Management Protocol*) - pozwala na zwielokrotnienie warstwy IrLAP. Ponadto umożliwia korzystanie z usług i protokołów zawartych w IAS (ang. *Information Access Service*).

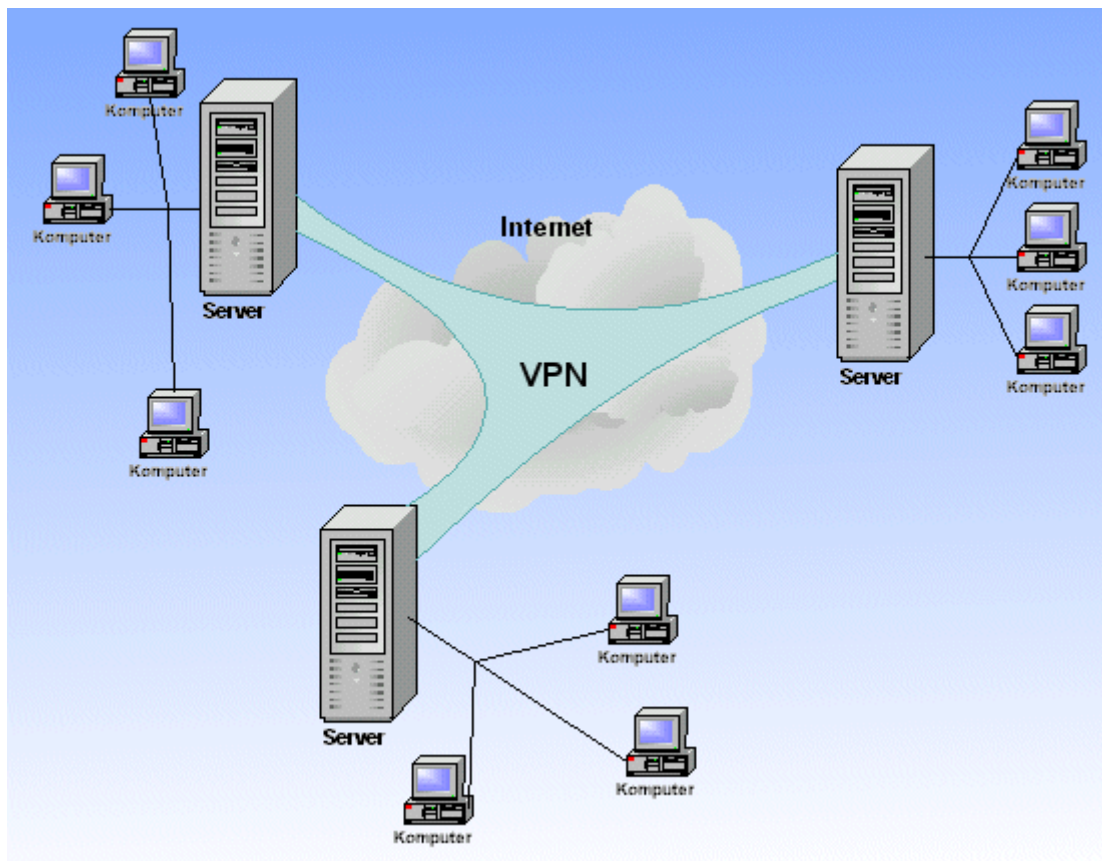
Protokoły opcjonalne przesyłu danych w standardzie IrDA to:

- **Tiny TP** - umożliwia niezawodną transmisję z wykorzystaniem protokołu IrLMP.
- **IrCOOM** - umożliwia emulację portów szeregowych i równoległych.
- **IrTran-P** - protokół wykorzystywany przy przesyłaniu obrazów.
- **IrMC** - opisuje standardy wymiany danych z telefonią komórkową, a także innymi urządzeniami służącymi do cyfrowej komunikacji.
- **IrLAN** - protokół pozwala na komunikację z siecią LAN, połączenie może odbywać się poprzez urządzenie dostępowe lub inny komputer dołączony już do sieci LAN.

Kompatybilność wszystkich połączonych urządzeń poprzez złącza IrDA możliwa jest dzięki wspólnym protokołom warstwy fizycznej i łącza danych.

(4.6) VPN

Wirtualna sieć prywatna VPN (ang. *Virtual Private Network*) to sieć umożliwiająca dwukierunkową transmisję danych, opartą na bazie sieci publicznej. VPN zapewnia ochronę danych poprzez przesyłanie ich w formie zaszyfrowanej. Istotą sieci VPN jest jednak fakt, że połączenie, choć odbywa się w ramach sieci publicznej (ogólnie dostępnej), jest realizowane tak, jak gdyby dotyczyło tylko wybranych komputerów odizolowanych od całej reszty sieci. Wyróżniamy dwa rodzaje połączeń VPN.



Rysunek 8.11. Tunele sieci VPN

Bezpieczny rękaw (ang. *secure sleeve*)

Przy przesyłaniu danych z użyciem tej techniki pakiet, który ma zostać wysłany, podlega zaszyfrowaniu, następnie kompresji, a później jest umieszczany w polu danych nowego pakietu, który zamiast adresu docelowego komputera zawiera adres docelowy routera, przez który docelowy komputer włącza się do sieci. Router po otrzymaniu danych ma możliwość dekompresji i rozszyfrowania ich. W ten sposób dowiaduje się gdzie ma wysłać pakiet. Tak więc stosując technikę bezpiecznego rękawa możemy ukryć strukturę sieci wewnętrznej.

Protokół tunelowania, używany przy *bezpiecznych rękawach*, to PPTP (ang. *Point-to-Point Tunneling Protocol*) firmy Microsoft. Użycie tego protokołu prowadzi do stworzenia tunelu do odbiorcy, którym najczęściej jest serwer NT/2000. Następnie przesyłane są pakiety PPP, ale tylko i wyłącznie z użyciem tunelu. Sesja taka jest zrywana po zakończeniu transmisji wymaganych pakietów przez docelowy NT/2000 serwer. Warto jeszcze nadmienić, że szyfrowanie odbywa się z wykorzystaniem metody klucza publicznego.

Bezpieczny tunel (ang. *secure tunnel*)

Podobnie jak przy wykorzystaniu poprzedniej techniki, przy przesyłaniu danych pakiet, który ma zostać wysłany podlega zaszyfrowaniu, następnie kompresji. Jedyną różnicą polega na tym, że nie jest szyfrowany nagłówek pakietu, a więc i adres docelowy komputera przeznaczenia. Należy pamiętać, że po ustanowieniu połączenia, dane są opakowywane w celu niemożności ingerencji w ich treść nawet wtedy, gdy pakiet podróżuje przez podsieci nie zapewniające mechanizmów bezpieczeństwa.

[NASTĘPNA](#)