Mikroserwery TCP/IP – podstawy TCP/IP

1. Informacje ogólne

Siecią komputerową można nazwać wszystko, co pozawala dwóm, bądź większej liczbie komputerów komunikowanie się ze sobą, lub z innymi urządzeniami. Dzięki sieciom można wykorzystać komputery do współużytkowania informacji, współpracy przy realizacji zadań, do drukowania, wymiany poczty elektronicznej, wymiana plików, itp.

Sieci składają się z wielu elementów, są to **sprzęt** oraz **oprogramowanie**.

Podstawowe sprzętowe składniki niezbędne do funkcjonowania wszelkiego rodzaju sieci to:

- urządzenia transmisji,
- urządzenia dostępu,
- urządzenia wzmacniania przesyłanych sygnałów (wzmacniaki).

Urządzenia transmisji są stosowane do transportu sygnałów biegnących przez sieć do miejsc docelowych. Takimi nośnikami są kable koncentryczne, skrętka dwużyłowa, kable światłowodowe (nośniki sieci lokalnej (LAN – Local Area Network) mogą być również niematerialne, np. powietrze, które przesyła światło, fale radiowe, mikrofale).

Urządzenia dostępu są odpowiedzialne za:

- formatowanie danych w taki sposób, aby nadawały się one do przesyłania w sieci,
- umieszczanie w sieci tak sformatowanych danych,
- odbieranie danych do nich zaadresowanych.

W sieci LAN urządzeniami dostępu są między innymi karty sieciowe. Karta taka pełni funkcję portu, za pomocą którego komputer przyłączony jest do sieci. Karty sieciowe oprawiają dane w ramki, których wysłania domagają się aplikacje komputera, po czym umieszczają te dane, które mają postać binarną, w sieci, a także odbierają ramki zaadresowane do obsługiwanych przez nie komputerów.

W sieciach rozległych (WAN – Wide Area Network) urządzeniami dostępu są routery. Działają one na poziomie warstwy sieci modelu OSI i składają się z protokołów dwojakiego rodzaju: protokołów trasowania i protokołów trasowalnych. Protokoły trasowalne, takie jak protokół IP, używane są do transportowania danych poza granice domen warstwy łącza danych. Protokoły trasowania udostępniają wszystkie funkcje niezbędne do:

- określania w sieci WAN ścieżek optymalnych dla każdego adresu docelowego,
- odbierania pakietów i przesyłanie ich dalej do miejsca docelowego z wykorzystaniem ścieżek.

Wzmacniak jest urządzeniem, które odbiera przesyłane sygnały, wzmacnia je i wysyła z powrotem do sieci. W sieciach LAN wzmacniak - częściej zwany **koncentratorem** - umożliwia przyłączanie do sieci wielu urządzeń. Generalnie ważną funkcją koncentratorów jest regenerowanie sygnałów. Sygnały elektroniczne umieszczone w sieci ulegają zakłóceniom:

- tłumienia,
- zniekształcenia.

Tłumienie można eliminować zmniejszając długość kabli na tyle, by moc sygnału umożliwiała mu dotarcie do wszystkich części okablowania. Jeśli kabel musi być długi, można na kablu zamocować wzmacniak. Zniekształcenia powodują większy problem

związany z przesyłaniem sygnałów. Wzmacniaki nie potrafią rozróżniać sygnałów prawidłowych od zniekształconych i wzmacniają wszystkie sygnały.

Składnikami programowymi niezbędnymi do utworzenia sieci są:
- protokoły - określają sposoby komunikowania się urządzeń,
- programy poziomu sprzętowego, nazywane mikroprogramami, sterownikami lub programami obsługi, czyli umożliwiają działanie urządzeniom, takim jak np. karty sieciowe.

Sterownikiem urządzeń określa się program, który umożliwia sterowanie określonym urządzeniem, można go porównać do miniaturowego systemu operacyjnego obsługującego jedno urządzenie. Sterownik karty sieciowej dostarcza interfejsu dla systemu operacyjnego hosta.

Oprogramowanie komunikacyjne pozwala korzystać z pasma przesyłania utworzonego i udostępnionego przez składniki sieci. Przykładami takich programów komunikacyjnych są programy mapowania dysków, sieć WWW, telnet, ftp, a nawet poczta elektroniczna.

Magistrala sieci LAN jest siecią, która do komunikacji w sieci używa karty interfejsu sieciowego (karty sieciowej). Magistralowa sieć lokalna składa się z następujących elementów składowych:
- medium transmisyjnego, czyli nośnika (magistrala),
- interfejsu fizycznego lub nadajnika - odbiornika dla każdego urządzenia przyłączanego do sieci,
- protokoły transmisji i komunikacji,
- oprogramowania umożliwiającego użytkownikom komunikowanie się i udostępnianie zasobów.

1.1. Pojęcia podstawowe z zakresu sieci komputerowych

Pakiet – „paczka danych” przesyłana między urządzeniami przy wykorzystaniu łącza komunikacyjnego (sieciowego); zawiera nagłówek i dane.

Protokół – sposób komunikowania się z innym systemem; zbiór zasad określających zachowanie się partnerów w komunikacji; określa parametry czasowe dla poszczególnych sygnałów oraz strukturę danych.

Przełącznik (*ang. switch*) - działanie podobne do koncentratora. Obsługuje łącza przełączane (większa wydajność).

Ramka – sekwencja bitów przesyłany przez łącze fizyczne.

Repeater – proste urządzenie pomocnicze, którego zadaniem jest regeneracja sygnału przesyłanego kablem. Pozwala to na zwiększenie długości połączenia, co w efekcie przyczynia się do zwiększenia rozpiętości sieci.

Router - sieciowe urządzenie trasujące (przekaźnik), odpowiedzialne za przesyłanie pakietów informacji między dwoma odległymi od siebie komputerami. Routerem może być zarówno komputer z zainstalowanym odpowiednim oprogramowaniem jak i opracowane specjalnie do tego celu urządzenie elektroniczne.

Topologia sieci - sposób fizycznego połączenia komputerów w jeden zespół.

DTE (data terminal equipment) - urzadzenie terminalowe danych lub inaczej stacja, jest unikalnym, zaadresowanym urządzeniem w sieci.

Urządzenie nadawczo-odbiorcze (transceiver) – urządzenie, które umożliwia stacji transmisje „do” i „z” któregoś ze standartowych mediów normy IEEE

802.3. Dodatkowo transceiver Ethernetowy zapewnia izolację elektryczną pomiędzy stacjami oraz wykrywa i reaguje na kolizje.

MAU (Medium Attachement Unit) moduł dołączania medium jest jednym z określeń IEEE na transceiver. Karta sieciowa najczęściej ma zintegrowany wewnątrz transceiver.

AUI (Attachment Unit Interface) - połączenie pomiędzy kontrolerem i transceiverem. Aktualnie prawie nie występuje, był to rodzaj kabla i gniazdek, do komunikowania się karty sieciowej z dołączanymi do niej transceiverami. Dopiero transceiver mógł zostać podłączony do medium transmisyjnego (np.: koncentryk, skrętka)

Segment – część okablowania sieci ograniczona przez mosty (bridge), przełączniki (switche), rutery, wzmacniaki lub terminatory. Najczęściej połączenie między dwoma komputerami lub koncentratorem i komputerem (dla skrętki i światłowodu), lub jeden odcinek kabla koncentrycznego łączącego wiele urządzeń.

Wzmacniak (repeater) – stanowi połączenie elektryczne między dwoma segmentami sieci. Jego zadaniem jest wzmocnienie i odnowienie sygnału w celu zwiększenia rozległości sieci. W żaden sposób nie ingeruje w zawartość logiczną ramki.

Koncentrator (hub, concentrator) – umożliwia podłączenie (w topologii gwiazdy) wielu urządzeń sieciowych w jeden segment. W rozważaniach można go traktować jak połączenie wielu wzmacniaków (wieloportowy wzmacniak).

2. Warstwowy model sieci komputerowej ISO – OSI (International Standard Organization - Open Systems Interconnection)

W 1977 roku „Międzynarodowa Organizacja Normalizacji ISO "International Organization for Standardization" www.iso.org opracowała wzorcowy „Model łączenia systemów otwartych” (Open System Interconnection). Ideą przyświecającą tym działaniom, było umożliwienie współdziałania ze sobą produktów pochodzących od różnych producentów.

Proces komunikacji został podzielony na 7 etapów, zwanych warstwami, ze względu na sposób przechodzenia pomiędzy nimi informacji. Często struktura tworzona przez warstwy OSI nazywana jest stosem protokołów wymiany danych. Warstwy od 1 do 3 umożliwiają dostęp do sieci, a warstwy od 4 do 7 obsługują komunikację końcową.

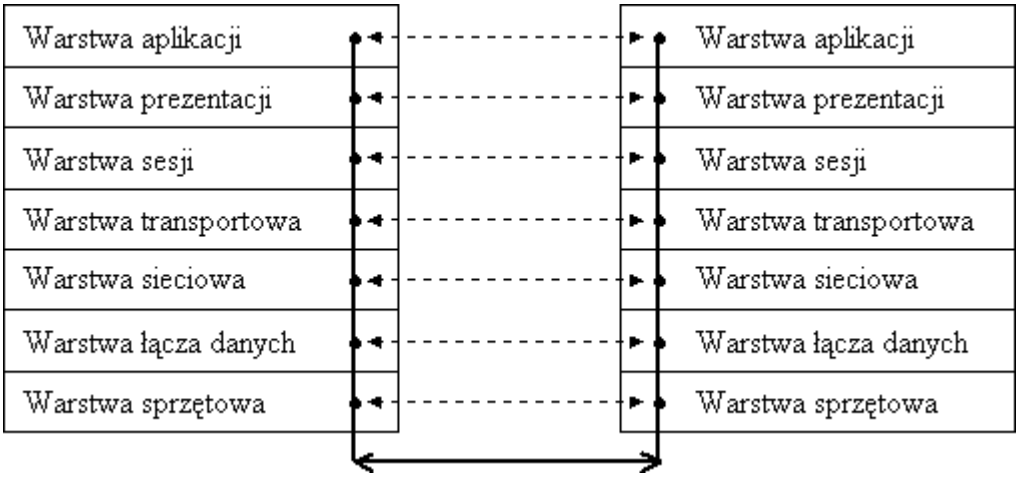
W złożonym zagadnieniu komunikacji wyodrębnia się pewne niezależne zadania, które mogą być rozwiązywane przez wydzielone układy sprzętowe lub pakiety oprogramowania zwane obiektami. Klasę obiektów rozwiązujących dane zagadnienie nazywa się **warstwą**. Pojęcie warstwy nie jest jednoznaczne z pojęciem protokołu – funkcje danej warstwy mogą być wykonywane przez kilka różnych protokołów. Każdy protokół komunikuje się ze swoim odpowiednikiem, będącym implementacją tego samego protokołu w równorzędnej warstwie komunikacyjnej systemu odległego. Warstwy (a dokładnie konkretne protokoły zawarte w tej warstwie) komunikują się bezpośrednio z odpowiadającymi im warstwami w odległym hoście. Należy więc też zapewnić reguły przekazywania informacji w dół do kolejnych warstw pracujących na danym komputerze. Dane przekazywane są od wierzchołka stosu, poprzez kolejne warstwy, aż do warstwy fizycznej, która przesyła je poprzez sieć do odległego hosta. Na szczycie stosu znajdują się usługi świadczone bezpośrednio użytkownikowi przez aplikacje sieciowe, na spodzie – sprzęt realizujący transmisję sygnałów niosących informacje.

Każda kolejna warstwa musi jedynie znać format danych wymagany do komunikacji poprzez warstwę niższą zwany protokołem wymiany danych. Przy przechodzeniu do warstwy

niższej dana warstwa dokleja do otrzymanych przez siebie danych nagłówek z informacjami dla swojego odpowiednika na odległym hoście. W ten sposób kolejne warstwy nie ingerują w dane otrzymane z warstwy poprzedniej. Przy odbieraniu danych z warstwy niższej, dana warstwa interpretuje ten nagłówek „doklejony" poprzez swojego odpowiednika i jeśli zachodzi potrzeba przekazania danych do warstwy wyższej, usuwa swój nagłówek i przekazuje dane dalej.

Tabela 1. Numeracja i nazwy warstw modelu OSI

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



Rys. 1. Transmisja danych pomiędzy kolejnymi warstwami ISO – OSI

Warstwa fizyczna (sprzętowa)

Warstwa najniższa nazywana jest **warstwą fizyczną**. Jest ona odpowiedzialna za przesyłanie strumieni bitów. Odbiera ramki danych z warstwy 2, czyli warstwy łącza danych, i przesyła szeregowo, bit po bicie, całą ich strukturę oraz zawartość. Jest ona również odpowiedzialna za odbiór kolejnych bitów przychodzących strumieni danych. Strumienie te są następnie przesyłane do warstwy łącza danych w celu ich ponownego ukształtowania.

Warstwa łącza danych

Druga warstwa modelu OSI nazywana jest warstwą **łącza danych**. Jak każda z warstw, pełni ona dwie zasadnicze funkcje: odbierania i nadawania. Jest ona odpowiedzialna za końcową zgodność przesyłania danych. W zakresie zadań związanych z przesyłaniem, warstwa łącza danych jest odpowiedzialna za upakowanie instrukcji, danych itp. W tzw. ramki. Ramka jest strukturą rodzimą - czyli właściwą dla - warstwy łącza danych, która zawiera ilość informacji wystarczającą do pomyślnego przesyłania danych przez sieć lokalną do ich miejsca docelowego. Pomyślna transmisja danych zachodzi wtedy, gdy dane osiągają miejsce docelowe w postaci niezmienionej w stosunku do postaci, w której zostały wysłane. Ramka musi więc zawierać mechanizm umożliwiający weryfikowanie integralności jej zawartości podczas transmisji.

W wielu sytuacjach wysyłane ramki mogą nie osiągnąć miejsca docelowego lub ulec uszkodzeniu podczas transmisji. Warstwa łącza danych jest odpowiedzialna za rozpoznawanie i naprawę każdego takiego błędu. Warstwa łącza danych jest również odpowiedzialna za ponowne składanie otrzymanych z warstwy fizycznej strumieni binarnych i umieszczanie ich w ramkach. Ze względu na fakt przesyłania zarówno struktury, jak i zawartości ramki, warstwa łącza danych nie tworzy ramek od nowa. Buforuje ona przychodzące bity dopóki nie uzbiera w ten sposób całej ramki.

Warstwa sieci

Warstwa sieci jest odpowiedzialna za określenie trasy transmisji między komputerem-nadawcą, a komputerem-odbiorcą. Warstwa ta nie ma żadnych wbudowanych mechanizmów korekcji błędów i w związku z tym musi polegać na wiarygodnej transmisji końcowej warstwy łącza danych. Warstwa sieci używana jest do komunikowania się z komputerami znajdującymi się poza lokalnym segmentem sieci LAN. Umożliwia im to własna architektura trasowania, niezależna od adresowania fizycznego warstwy 2. Korzystanie z warstwy sieci nie jest obowiązkowe. Wymagane jest jedynie wtedy, gdy komputery komunikujące się znajdują się w różnych segmentach sieci przedzielonych routerem.

Warstwa transportu

Warstwa ta pełni funkcję podobną do funkcji warstwy łącza w tym sensie, że jest odpowiedzialna za końcową integralność transmisji. Jednak w odróżnieniu od warstwy łącza danych - warstwa transportu umożliwia tę usługę również poza lokalnymi segmentami sieci LAN. Potrafi bowiem wykrywać pakiety, które zostały przez routery odrzucone i automatycznie generować żądanie ich ponownej transmisji. Warstwa transportu identyfikuje oryginalną sekwencję pakietów i ustawia je w oryginalnej kolejności przed wysłaniem ich zawartości do warstwy sesji.

Warstwa sesji

Piątą warstwą modelu OSI jest **warstwa sesji**. Jest ona rzadko używana; wiele protokołów funkcje tej warstwy dołącza do swoich warstw transportowych. Zadaniem warstwy sesji modelu OSI jest zarządzanie przebiegiem komunikacji podczas połączenia miedzy dwoma komputerami. Przepływ tej komunikacji nazywany jest sesją. Warstwa ta określa, czy komunikacja może zachodzić w jednym, czy obu kierunkach. Gwarantuje również zakończenie wykonywania bieżącego żądania przed przyjęciem kolejnego.

Warstwa prezentacji

Warstwa prezentacji jest odpowiedzialna za zarządzanie sposobem kodowania wszelkich danych. Nie każdy komputer korzysta z tych samych schematów kodowania danych, więc warstwa prezentacji odpowiedzialna jest za translację między niezgodnymi schematami kodowania danych. Warstwa ta może być również wykorzystywana do niwelowania różnic między formatami zmiennopozycyjnymi, jak również do szyfrowania i rozszyfrowywania wiadomości.

Warstwa aplikacji

Najwyższą warstwą modelu OSI jest **warstwa aplikacji**. Pełni ona rolę interfejsu pomiędzy aplikacjami użytkownika a usługami sieci. Warstwę tę można uważać za inicjującą sesje komunikacyjne.

Mimo, iż model składa się z siedmiu warstw, to określona sesja komunikacyjna nie musi wykorzystywać wszystkich siedmiu, lecz tylko niektóre z nich. Np., komunikacja w ramach

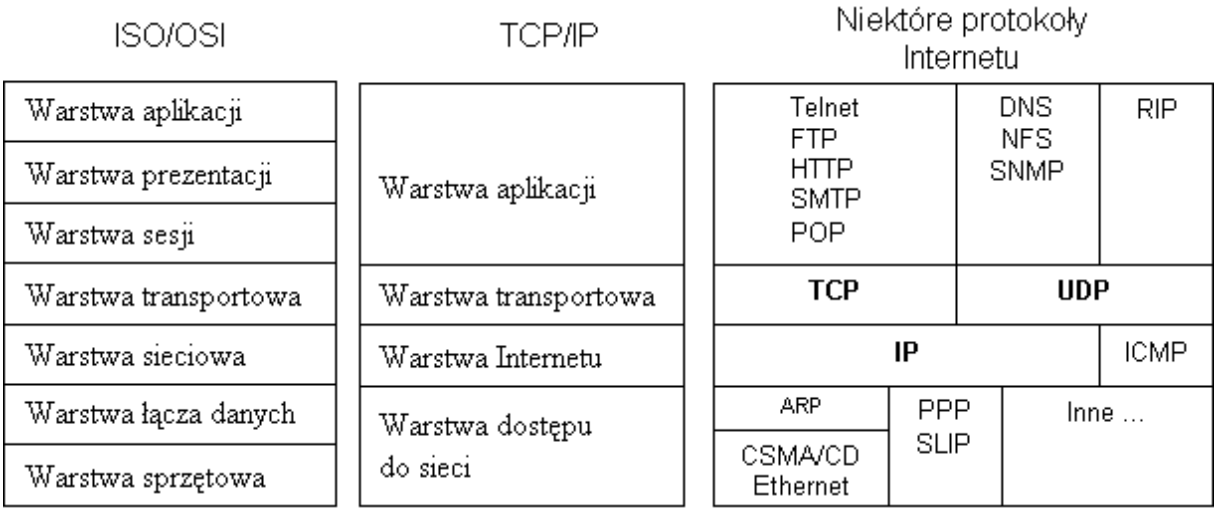
jednego segmentu LAN może być przeprowadzana wyłącznie w warstwach 1 i 2 modelu OSI, bez potrzeby korzystania z dwóch pozostałych (3 i 4) warstw komunikacyjnych.

Większość obecnie używanych protokołów używa własnych modeli warstwowych. Mogą one w różnym stopniu odpowiadać podziałowi funkcji określonemu przez model OSI. Modele te bardzo często dzielą funkcje nie między 7, lecz między 5 lub mniej warstw. Często też warstwy wyższe różnią się znacznie od ich odpowiedników modelu OSI.

3. Model protokołu TCP/IP

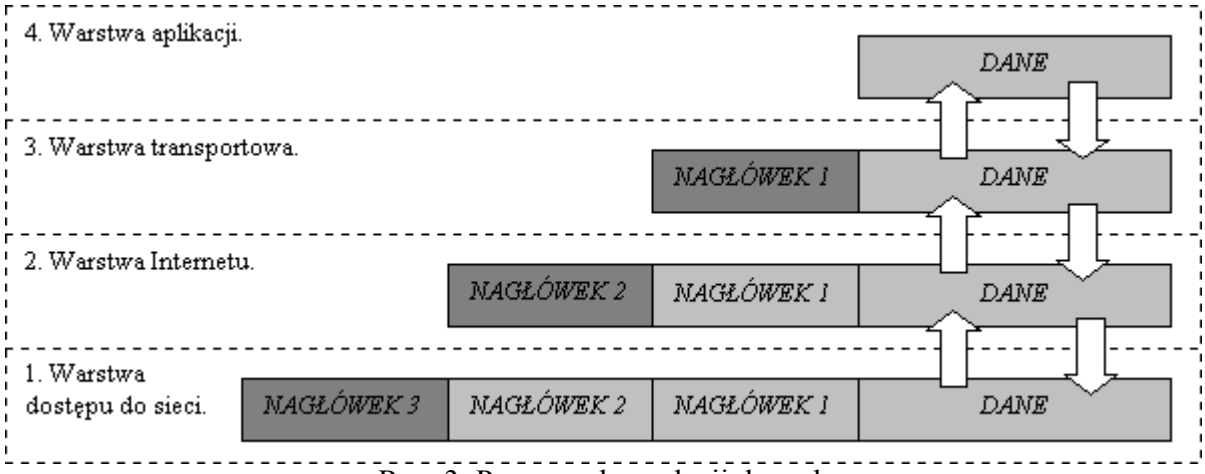
Protokół tworzący Internet - TCP/IP - również możemy opisać za pomocą siedmio-warstwowego modelu ISO – OSI. Lepiej jednak oddaje funkcje i właściwości protokołu TCP/IP uproszczony model cztero-warstwowy. W modelu tym najważniejsze są warstwy sieciowa i transportowa, pozostałe są połączone i tworzą dwie warstwy zwane warstwą dostępu do sieci oraz warstwą aplikacji. Funkcje tych warstw pokrywają się z zadaniami odpowiadających im warstw w modelu ISO – OSI (rys. 2).
Podsumowując protokół TCP/IP dzieli się na cztery warstwy (od najniższej):

- warstwa dostępu do sieci,
- warstwa internet (nazywana inaczej sieciową, międzysieciową lub warstwą IP),
- warstwa transportowa,
- warstwa zastosowań (nazywana inaczej warstwą aplikacji).



Rys. 2. Porównanie modelu ISO – OSI i modelu TCP/IP

Podobnie jak w modelu OSI kolejne warstwy dołączają (bądź usuwają, w zależności w którą stronę przesuwają się dane na stosie protokołów) własne nagłówki. Taki proces nazywa się **enkapsulacją** danych (rys. 3).

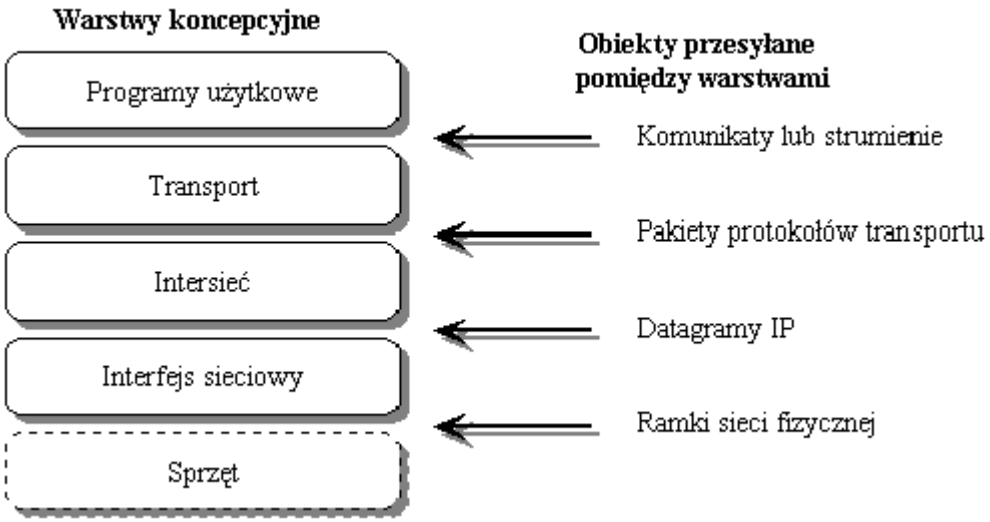


Rys. 3. Proces enkapsulacji danych

Każda warstwa ma swoją terminologię określającą dane aktualnie przez nią obrabiane. Ponieważ protokół TCP/IP składa się z dwóch głównych protokołów warstwy transportowej TCP i UDP, więc również w nazewnictwie wprowadzony został podział.

Tabela 2. Nazwy jednostek danych dla warstw modelu TCP/IP

Warstwa	**TCP**	**UDP**
Aplikacji	strumień	wiadomość
Transportowa	segment	pakiet
Internetu	datagram	
Dostępu do sieci	ramka	



Rys. 4. Obiekty przesyłane pomiędzy warstwami

Warstwa dostępu do sieci odpowiada za dostarczanie danych do innych urządzeń bezpośrednio dołączonych do sieci. Współpracuje ona bezpośrednio ze sprzętem i sterownikami odpowiedzialnymi za współpracę z siecią Ethernet. W przypadku innych sieci mogą to być protokoły PPP, SLIP lub inne. Warstwa ta współpracuje więc z interfejsem sieciowym (kartą sieciową), modemem lub innym urządzeniem pozwalającym na bezpośrednie połączenie dwóch lub więcej komputerów i separuje resztę warstw od zastosowanych rozwiązań fizycznych (niskopoziomowych). Świadczy ona usługę warstwie

wyższej polegającą na wysyłaniu i odbieraniu porcji danych (zwanych ramkami) z komputerów w danej sieci fizycznej.

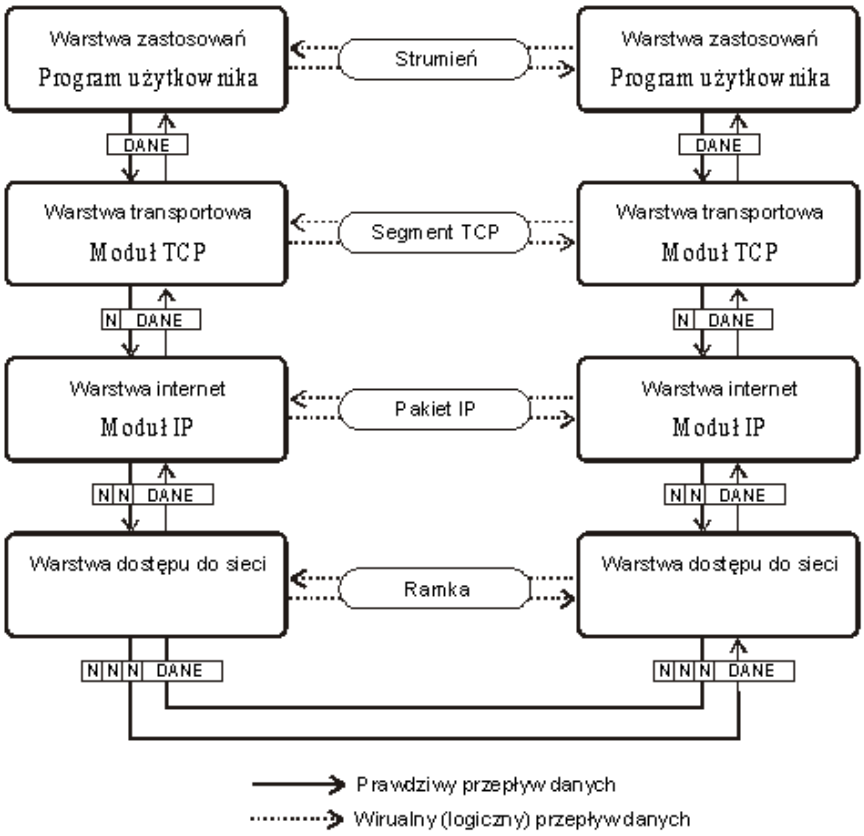
Warstwa internet (IP) odpowiada za dostarczanie danych do urządzeń nie tylko w danej sieci fizycznej. Organizuje ona ruch tzw. pakietów IP między poszczególnymi sieciami fizycznymi połączonymi w intersieć. Korzysta z usług warstwy dostępu do sieci, sama zaś świadczy usługi dostarczania pakietu do dowolnego komputera w Internecie.

Warstwa transportowa odpowiedzialna jest za niezawodną wymianę danych z dowolnym komputerem w Internecie. Organizuje też i utrzymuje tzw. sesje, czyli wirtualne połączenia między komputerami. Korzysta z warstwy IP, sama zaś dostarcza usług niezawodnego transportu danych.

Warstwa zastosowań jest najwyżej położona. Tej warstwie odpowiadają wszelkie programy (aplikacje) internetowe korzystające z warstwy transportowej. Tu znajdują się wszelkie konkretne zastosowania Internetu - przesyłanie plików (FTP), poczty (SMTP) i inne.

Współpraca między warstwami polega na świadczeniu usług przez warstwy niższe warstwom wyższym. Związane to jest także z przepływem danych w dół sterty warstw (przy wysyłaniu danych) i w górę (przy odbieraniu). Moduł warstwy zastosowań (najczęściej program użytkownika) wysyła dane do warstwy transportowej. Ta odpowiednio formatuje je (dzieli lub łączy, dodaje nagłówek) i wysyła do warstwy IP. Ta z kolei dodaje swój nagłówek i wysyła do warstwy dostępu do sieci. I ta warstwa dołącza swój nagłówek (związany ze sprzętowym rozwiązaniem komunikacji, np. tzw. nagłówek MAC) i wysyła pakiet fizycznie do sieci.

Podobna droga, ale w drugą stronę, czeka dane w komputerze je odbierającym. Pakiet wędruje ku górze i jest pozbawiany odpowiednich nagłówków, by wreszcie dotrzeć do warstwy zastosowań w formie identycznej porcji danych jaką wysłała warstwa zastosowań w komputerze wysyłającym. Przedstawiony wyżej opis jest faktycznym obiegiem danych.



Rys. 5. Współpraca między warstwami w TCP/IP

W koncepcji warstw istnieje jeszcze coś takiego jak wirtualny (logiczny) obieg danych. Występuje on pomiędzy odpowiadającymi sobie warstwami w odległych systemach. Warstwy dostępu do sieci wymieniają między sobą ramki. Warstwy IP wysyłają do siebie pakiety IP - choć w rzeczywistości muszą się ze sobą komunikować poprzez swoje niższe warstwy, to z logicznego punktu widzenia istnieje między nimi wirtualne połączenie, które pozwala na wymianę pakietów. Podobnie jest z warstwami transportowymi, które wysyłają między sobą poprzez swój wirtualny kanał pakiety danych (segmenty TCP) i inne komunikaty zapewniające utrzymanie sesji i niezawodne dostarczenia danych (potwierdzanie).

Między warstwami zastosowań istnieje również wirtualny kanał pozwalający na wysyłanie strumienia danych w obie strony. Tę warstwę stanowią najczęściej programy Internetowe i z ich punktu widzenia istnieje bezpośrednie połączenie strumieniowe z innym programem działającym na komputerze odległym. Dzięki temu programista nie musi znać budowy i zasady działania warstw niższych - musi jedynie poznać usługi świadczone przez warstwę transportową.

4. Ethernet

Ethernet (obecnie Ethernet II) jest techniką sieciową o topologii szynowej. Metodologia dostępu do nośnika, zastosowana w Ethernecie II, nazwana została wielodostępem do łącza sieci z badaniem stanu kanału i wykrywaniem kolizji CSMA/CD. Ethernet jest bogatym i różnorodnym zbiorem technologii. Sieci Ethernet mogą pracować w paśmie podstawowym lub mogą być szerokopasmowe, pełno dupleksowe lub półdupleksowe. Mogą wykorzystywać jeden z pięciu różnych nośników i pracować z prędkościami z zakresu od 10 Mbps do 1Gbps.

Na sprzęt, który może być używany do obsługi sieci Ethernet, składają się:

- karty sieciowe,
- koncentratory wzmacniające,
- koncentratory nie wzmacniające,
- mosty,
- routery.

Specyfikacje serii IEEE 802, w których zawiera się specyfikacja Ethernet, dzielą warstwę łącza danych modelu OSI na dwie odrębne części. Ich nazwy pochodzą od nazw kontrolowanych przez nie funkcji. Są to:

- sterownie łączem logicznym (LLC - LOGICAL LINK CONTROL),
- sterowanie dostępem do nośnika (MAC - MEDIA ACCESS CONTROL).

Wspólnie warstwy LLC i MAC tworzą jądro Ethernetu. Umożliwiają one umieszczanie danych w ramkach oraz adresowanie ich, co pozwala na przesyłanie ich do miejsca przeznaczenia.

Warstwa LLC jest wyższym z dwóch składników warstwy łącza danych. Izoluje ona protokoły wyższej warstwy od właściwej metody dostępu do nośnika. Sterownie łączem danych jest mechanizmem uniezależniającym protokoły warstw sieci i transportu od różnych odmian architektury sieci LAN. Dzięki temu protokoły wyższych warstw nie muszą wiedzieć, czy będą przesyłane poprzez Ethernet, Token Ring czy też Token Bus. Nie musza również wiedzieć, jakiej specyfikacji warstwy fizycznej będą używać. Sterownie LLC udostępnia wspólny interfejs dla wszystkich architektur i odmian sieci LAN zgodnych ze specyfikacją 802.

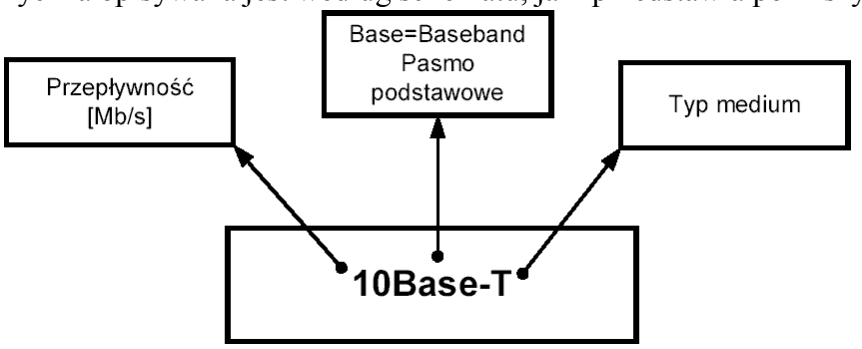
Warstwa MAC jest niższym składnikiem warstwy łącz danych w architekturze IEEE. Odpowiada ona za połączenie z warstwą fizyczną oraz zapewnia udany przebieg nadawania i odbioru. Składają się na nią dwie funkcje: **nadawania** i **odbioru**.

Warstwa sterownia dostępem do nośnika odpowiada za opakowywanie wszystkich danych otrzymanych z warstwy LLC w ramki. Prócz danych ramka zawiera strukturę oraz wszystkie adresy potrzebne do przesłania jej do miejsca przeznaczenia. Warstwa MAC jest także odpowiedzialna za przeprowadzanie testu integralności danych, używanego do sprawdzania, czy zawartość ramki nie została uszkodzona lub zmieniona podczas transmisji.

Warstwa sterowania dostępem do nośnika zawiera również mechanizmy potrafiące określać - na podstawie mechanizmów warstwy fizycznej - czy pasmo komunikacyjne jest dostępne, czy też nie. Jeśli jest dostępne, ramki danych są przekazywane warstwie fizycznej do przesłania. Jeśli nie, warstwa MAC uruchamia swój binarny wykładniczy algorytm zwrotny, który generuje pseudolosowy czas oczekiwania, po upływie którego dopiero może nastąpić kolejna próba transmisji.

Ostatnią ważną funkcją warstwy sterowania dostępem do nośnika jest monitorowanie statusu transmitowanych ramek polegające na wykrywaniu wszelkich znaków sygnalizujących zajście konfliktu. Gdy warstwa MAC wykryje konflikt jednej ze swoich ramek, określa, które dane muszą być ponownie wysłane, uruchamia algorytm zwrotny i ponownie próbuje wysłać ramkę. Algorytm zwrotny jest powtarzany, dopóki próba wysłania ramki nie zakończy się powodzeniem.

Warstwa fizyczna opisywana jest według schematu, jaki przedstawia poniższy rysunek:



Rys. 6. Opis elementów w nazwie technologii

W standardzie IEEE 802.3 wymieniane są trzy podstawowe odmiany sieci, w których zastosowane jest różne okablowanie:

- **10Base2**, wywodzi swoją nazwę z następującej konwencji: szybkości sygnału (w Mbps) + metoda transmisji (transmisja pasmem podstawowym) + maksymalna długość kabla w metrach, zaokrąglona do 100, a następnie podzielona przez 100. Sieci 10Base2 mogą być rozszerzane poza granicę 185 metrów za pomocą wzmacniaków, mostów lub routerów. Używając routerów do segmentacji Etherntetu, tworzy się segmenty 10Base2, które mogą być rozgałęziane do 30 razy, przy czym każde z rozgałęzień może obsłużyć do 64 urządzeń. W tej odmianie sieci stosuje się cienki kabel (kabel koncentryczny o średnicy 5mm).
- Interfejs **10Base5** wykorzystuje dużo grubszy kabel koncentryczny niż 10Base2 (kabel koncentryczny o średnicy 10 mm i impedancji 50 omów). Skuteczność transmisji w przewodzie miedzianym jest bowiem funkcją grubości przewodnika. Im większa jest jego średnica, tym większą osiąga się szerokość pasma. W rezultacie, kabel 10Base5 może być rozgałęziany do 100 razy, przy zachowaniu maksymalnej liczby 64 urządzeń dla każdego rozgałęzienia.
- Specyfikacja **10BaseT**, wbrew powszechnemu przekonaniu, nie określa rodzaju użytego kabla. Dotyczy ona natomiast specjalnej techniki sygnalizowania dla nieekranowanej skrętki dwużyłowej (UTP – Unshielded twisted-pair cable) wykorzystującej cztery przewody spełniające wymogi trzeciej kategorii wydajności. Nazwy przewodów wskazują

na ich funkcje oraz biegunowość. Jedna para przewodów obsługuje dodatnie i ujemne bieguny obwodu nadawania. Druga para obsługuje dodatnie i ujemne bieguny obwodu odbioru. Wzmacniaki/koncentratory 10BaseT używają przyporządkowań wyprowadzeń, które umożliwiają tworzenie łączy z portami kart sieciowych. W normalnych warunkach urządzenie końcowe zawsze jest połączone z urządzeniem komunikacyjnym. Komplementarność interfejsów tych urządzeń pozwala łączyć je bezpośrednio za pomocą kabla, bez obaw o konflikty miedzy nadawaniem i odbiorem. Sieć oparta na specyfikacji 10BaseT wykonana jest w topologii gwiazdy, co wymaga zastosowania koncentratora lub huba. Maksymalna długość segmentu wykonanego ze skrętki wynosi 100m. W przypadku konieczności użycia dłuższego segmentu trzeba zastosować wzmacniak. Maksymalna liczba węzłów roboczych przyłączonych do jednego segmentu wynosi 1024. Jednocześnie jest to maksymalna liczba węzłów, które mogą występować w całej tej sieci.

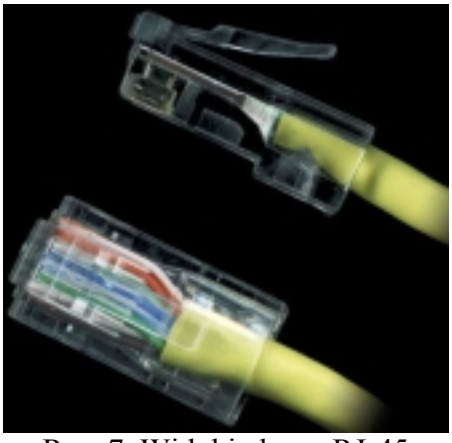
4. 1. Okablowanie dla specyfikacji 10BaseT

W specyfikacji 10BaseT stosuje się nieekranowaną skrętkę dwużyłową (UTP) kategorii 3, co nie znaczy, że nie można stosować lepszych kabli (kategorii 4 i 5). Poniżej podano parametry elektryczne skrętek UTP.
Częstotliwość przenoszonego sygnału:

- Skrętka UTP-3 do 16MHz,
- Skrętka UTP-4 do 20MHz,
- Skrętka UTP-5 do 100MHz.

Rezystancja: skrętka UTP-3, 4, 5 - 9,4 Ω/100m.
Impedancja: skrętka UTP-3, 4, 5 - 100 Ω.

Kable w sieci Ethernet specyfikacji 10BaseT zakończone są końcówką RJ-45 (ośmiopozycyjnym łącznikiem modularnym) (rys. 7).

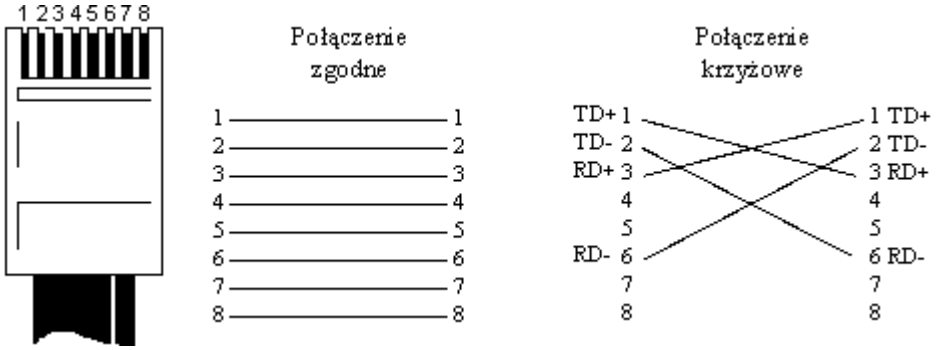


Rys. 7. Widoki złącza RJ-45

Wyróżniamy 3 rodzaje połączeń końcówek kabla UTP:

- odwrotny - końcówka 1 do 8, końcówka 7 do 2, itd. – zastosowany w kablu telefonicznym,
- zgodny - końcówka 1 do 1, końcówka 2 do 2, itd. – np.: połączenie Ethernet pomiędzy koncentratorem i kartą sieciową komputera,

- krzyżowy - (cross-over) odwraca tylko niektóre połączenia, często spotykane przy połączeniach pomiędzy koncentratorami lub przy łączeniu dwóch komputerów bez pośrednictwa koncentratora.



Rys. 8. Połączenie zgodne i krzyżowe kabla UTP

Tabela 3. Połączenie zgodne UTP

Przeznaczenie	**Nr**	**Kolor**	**Nr**	**Przeznaczenie**
Odbiór +	1	Biało/Pomarańczowy	1	Transmisja +
Odbiór -	2	Pomarańczowy	2	Transmisja -
Transmisja +	3	Biało/Zielony	3	Odbiór +
(nie używane)	4	Niebieski	4	(nie używane)
(nie używane)	5	Biało/Niebieski	5	(nie używane)
Transmisja –	6	Zielony	6	Odbiór -
(nie używane)	7	Biało/Brązowy	7	(nie używane)
(nie używane)	8	Brązowy	8	(nie używane)

Tabela 4. Połączenie krzyżowe UTP

Przeznaczenie	**Nr**	**Kolor**	**Nr**	**Przeznaczenie**
Transmisja +	3	Biało/Zielony	1	Odbiór +
Transmisja -	6	Zielony	2	Odbiór -
Odbiór +	1	Biało/Pomarańczowy	3	Transmisja +
(nie używane)	7	Biało/Brązowy	4	(nie używane)
(nie używane)	8	Brązowy	5	(nie używane)
Odbiór -	2	Pomarańczowy	6	Transmisja -
(nie używane)	4	Niebieski	7	(nie używane)
(nie używane)	5	Biało/Niebieski	8	(nie używane)

4.2. Sygnały i ich kodowanie

Sygnały w 10Mbps są kodowane za pomocą schematu kodowania **Manchester**. W schemacie tym sygnały zegara i danych są połączone i w środku każdego bitu następuje przeskok taktu. Zasady kodowania Manchester:

- 0 - sygnał o wysokiej wartości w pierwszej połowie okresu i niskiej w drugiej,
- 1 - sygnał o niskiej wartości w pierwszej połowie okresu i wysokiej w drugiej.

Sygnały w skrętce dla 10Base-T mają poziomy napięć od **-2,5V** do **+2,5V**, przy standardzie 100Base-T od -1V do +1V.

4.3. Adresy MAC

Adresy MAC *(Media Access Contro*l) są podzbiorem adresów warstwy 2 modelu OSI. Adres MAC ma 48 bitów (6 oktetów). Składa się z dwóch podstawowych części: w pierwszej zapisany jest kod producenta karty sieciowej przydzielany przez IEEE, w drugiej – unikatowy adres karty sieciowej tego producenta.

Adres MAC służy do jednoznacznej identyfikacji konkretnej karty sieciowej w sieci lokalnej i może być wykorzystany np. do ograniczenia dostępu konkretnych maszyn z tejże sieci do Internetu udostępnianego za pomocą maskarady pracującej pod systemem uniksowym.

Pod adresem http://standards.ieee.org/regauth/oui/oui.txt można znaleźć spis wszystkich MAC-adresów przyporządkowanych poszczególnym producentom.

Pierwsze trzy oktety identyfikują producenta sprzętu, np:

- 00-AA-00 to Intel,
- 00-20-AF to 3Com,
- 00-00-0C to Cisco.

Pozostałe 3 oktety przyznaje producent. 3 oktety umożliwiają przydzielenie ponad 16 mln. adresów. Niektórzy producenci sprzedali już ponad 16 mln. urządzeń i postarali się w IEEE o nowe identyfikatory.

5. Warstwa internetu TCP/IP

Składa się ona z dwóch protokółów:

- IP - Internet Protocol - jest protokołem warstwy sieciowej, oddziela on wyższe warstwy od znajdującej się poniżej sieci i obsługuje adresowanie i dostarczanie danych.
- TCP - Transmission Control Protocol - jest protokołem warstwy transportowej, gwarantuje, że odbiorca otrzyma dane dokładnie w tej samej postaci, w jakiej zostały wysłane.

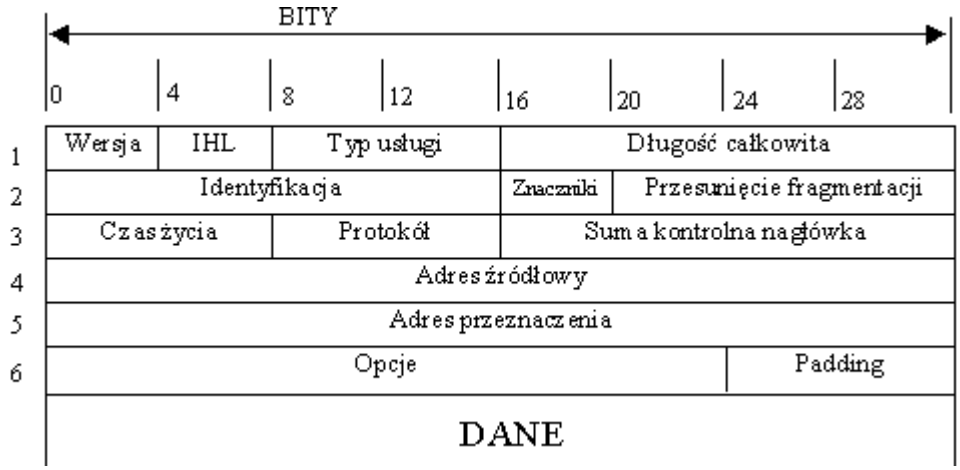
5.1. Protokół IP

IP jest bezpołączeniowym protokołem komunikacyjnym, generującym usługi **datagramowe**. Znaczy to, że sieć oparta na tym protokole jest siecią z przełączaniem pakietów. Pakiet rozumiemy tu jako blok danych uzupełniony o informacje niezbędne do jego prawidłowego dostarczenia (nagłówki i końcówki). Sieć z przełączaniem pakietów wykorzystuje informację adresową do przełączania pakietów z jednej sieci fizycznej do drugiej, aż do miejsca przeznaczenia. Każdy pakiet jest przesyłany po sieci w sposób niezależny. Należy sobie uświadomić, że jeśli pewna porcja danych została podzielona na pakiety i wysłana do pewnego adresata, to droga każdego z tych pakietów przez sieć do adresata może okazać się całkiem inna. Przepływ pakietów (datagramów) w sieci odbywa się bez kontroli kolejności dostarczania ich do miejsca przeznaczenia, kontroli błędów i bez potwierdzania odbioru. Dzięki takiemu ograniczeniu funkcji, jakie musi spełniać IP, powoduje jego szybkość i efektywność.

W sieciach z protokołem IP przepływem datagramów sterują routery IP. Routery IP łączą sieci lokalne lub zdalne przesyłając datagramy pomiędzy nimi.

Przekierowanie datagramu odbywa się ze względu na numer logiczny jego adresata. Numer logiczny nazywa się w tym protokole numerem IP.

Datagram jest to format pakietu zdefiniowanym przez protokół Internet. Na rys. 9 znajduje się graficzna reprezentacja datagramu IP.



Rys. 9. Graficzna reprezentacja datagramu IP

Wersja – [4 bity] – numer wersji protokołu IP. Opisana została wersja nr 4.
IHL – [4 bity] – (Internet Header Length) jest długością nagłówka w słowach. Minimalna wartość to 5.
Typ usługi – [8 bitów] – TOS (Type of Service) opisuje jakość wymaganej usługi. Kolejne bity oznaczają:
0-2: pierwszeństwo:
111 – sterowanie siecią,
110 – sterowanie siecią wewnętrzną,
101 – CRITIC/ECP,
100 – natychmiastowe zastąpienie,
011 – zastąpienie,
010 – natychmiastowe,
001 – priorytet,
000 – program standardowy,
3: opóźnienie, 0 – normalne, 1- małe,
4: wydajność, 0 – normalna, 1 – wysoka,
5: niezawodność, 0 – normalna, 1 – wysoka,
6-7: zarezerwowane do użycia w przyszłości.
Długość całkowita – [16 bitów] – jest długością pakietu IP w bajtach (zawierającego nagłówek i dane).
Identyfikator – [16 bitów] – wartość identyfikacyjna przypisana nadawanemu pakietowi przed fragmentacją (jeżeli miałaby ona miejsce). W przypadku fragmentacji określa ona przynależność fragmentu do datagramu.
Flagi – [3 bity] – flagi sterujące:
bit nr 0: - zarezerwowany, musi mieć wartość zero;
bit nr 1: DF - 0 – można fragmentować, 1- nie wolno fragmentować;
bit nr 2: MF - 0 – ostatnia fragmentacja, 1 - więcej fragmentacji.
Przesunięcie fragmentacji – [13 bity] – pole to wskazuje, do którego miejsca pakietu danych należy ten fragment. Przesunięcie fragmentu jest mierzone w jednostkach 8 bajtów (64 bitów). Pierwszy fragment ma przesunięcie równe zeru.
Czas życia – [8 bitów] – TTL - pole to wskazuje maksymalny czas przebywania pakietu w Internecie (Time-to-Live).
Protokół – [8 bitów] – pole to wskazuje numer protokołu warstwy wyższej, do którego zostaną przekazane dane z tego pakietu.

Suma kontrolna – [16 bitów] – suma kontrolna nagłówka. Ponieważ nagłówek ulega ciągłym zmianom (np. czas życia) jest ona obliczana i sprawdzana za każdym razem, gdy dany nagłówek jest przetwarzany.
Adres źródła – [32 bity] – adres IP źródła danych.
Adres przeznaczenia – [32 bity] – adres IP komputera docelowego.
Opcje – [długość pola jest zmienna] – mogą zajmować przestrzeń na końcu nagłówka IP.
Uzupełnienie – [długość pola jest zmienna] – jeśli pole opcji nie zajmuje pełnego słowa to zostaje uzupełnione do 32 bitów.

Protokół IP jest na tyle uniwersalny, że zapewnia transport danych przez różnorodne strukturalnie sieci (np. Token Ring, X.25). Każdy rodzaj sieci ma określony maksymalny rozmiar pakietu MTU (Maximum Transmission Unit). W trakcie przekazywania danych, może się okazać, że MTU właściwy dla jednej z sieci, jest zbyt duży dla następnej. Zachodzi wtedy zjawisko fragmentacji pakietu. W tym momencie rolę zaczynają odgrywać pola identyfikator, przesunięcie fragmentacji oraz pole flagi w nagłówku datagramu.
Numer protokołu

Pole protokół w nagłówku datagramu jest numerem protokołu, do którego mają zostać dostarczone dane z tego datagramu. Z numeru tego korzystają warstwy wyższe w celu identyfikacji protokołu, który zapewni dalszą obróbkę danych. W systemach Unixowych numery protokołów zapisane są w pliku /etc/protocols. Plik ten może wyglądać w podany poniżej sposób (Druga kolumna zawiera numer protokołu):

ip 0 IP # internet protocol, pseudo protocol number
icmp 1 ICMP # internet control message protocol
igmp 2 IGMP # internet group multicast protocol
ggp 3 GGP # gateway-gateway protocol
tcp 6 TCP # transmission control protocol
pup 12 PUP # PARC universal packet protocol
udp 17 UDP # user datagram protocol
idp 22 IDP # Internet Datagram Protocol
raw 255 RAW # RAW IP interface

5.1.1. Adresowanie IP

Adresy wszystkich komputerów w Internecie są wyznaczane przez właściwości protokołu IP. Z rys. 9 widzimy, że pola „Adres źródła" i „Adres przeznaczenia" składają się z czterech bajtów (oktetów) każde. Z tego wynika konstrukcja adresu Internetowego, który składa się z czterech liczb dziesiętnych z zakresu 0-255 przedzielonych kropkami. Można go również zapisać jako jeden ciąg 32 bitów lub też cztery ciągi po osiem bitów każdy, przedzielone kropkami.

Każdy taki adres można podzielić na dwie części:

- część identyfikującą daną sieć w Internecie,
- część identyfikującą konkretny komputer w tej sieci.

Podział ten wynika z faktu, że każde przedsiębiorstwo, które otrzymuje adresy internetowe do własnego wykorzystania, otrzymuje tylko jakiś wydzielony zakres tych adresów, określany mianem: przestrzeń adresowa.

Pierwotnie bity określające sieć i bity określające komputer były rozróżniane za pomocą tzw. **klas adresów** IP. Klasy były definiowane za pomocą kilku pierwszych bitów adresu. Na podstawie ich wartości oprogramowanie określało klasę adresu, a tym samym które bity odpowiadają za adres podsieci, a które za adres hosta:

0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh - klasa A

10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh - klasa B
110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh - klasa C
1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx - multicast
1111xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx - adresy zarezerwowane

gdzie|: n – bit należący do adresu sieci, h – bit należący do adresu hosta.

W ten sposób, na podstawie wartości N pierwszego bajtu adresu IP możemy zdefiniować do jakiej klasy należy dany adres:

N < 128 – klasa A
128 < N < 191 – klasa B
192 < N < 223 – klasa C
224 < N < 239 – multicast
N > 239 – adresy zarezerwowane

Adresy multicast są adresami transmisji grupowej, wykorzystywanymi przy np.: wideo-konferencjach.

Maska sieci składa się podobnie jak adres IP z 4 bajtów, używana jest do wydzielenia części adresu odpowiadającej za identyfikację sieci i części odpowiadającej za identyfikację komputera z adresu IP. Poniżej zamieszczam ilustrację tej metody.

Adres IP: 212.51.219.50
Maska sieci: 255.255.255.192
Adres sieci: 212.51.219.0
Broadcast: 212.51.219.63

Adres sieci tworzymy przepisując niezmienione wszystkie bity adresu IP, dla których odpowiednie bity maski mają wartość jeden. Resztę uzupełniamy zerami. Adres broadcast jest adresem **rozgłoszeniowym** sieci. Używa się go do jednoczesnego zaadresowania wszystkich komputerów w danej sieci (jest przetwarzany przez wszystkie komputery w sieci). Tworzymy go podobnie do adresu sieci, jednak dopełniamy jedynkami zamiast zerami.

Mając adres sieci i adres broadcast możemy łatwo wyznaczyć możliwy zakres numerów IP komputerów w danej sieci. Dla podanych powyżej adresów sieci i broadcast, komputerów w sieci mogą przyjmować adresy IP od numeru: 212.51.219.1 do 212.51.219.62.

Adres 212.51.219.50 z maską 255.255.255.192 możemy w skrócie zapisać 212.51.219.50/26. W tym przypadku ostatnia liczba oznacza ilość bitów o wartości jeden w masce.

Istnieją pewne adresy, których nie można wykorzystać do normalnych zastosowań (przydzielić ich komputerom). Dla danej sieci (przestrzeni adresowej) takim adresem jest adres sieci. W omawianym przykładzie tym adresem jest 212.51.219.0; adres ten symbolizuje całą sieć. Drugim takim adresem jest wyznaczony powyżej broadcast, czyli adres rozgłoszeniowy. Każdy datagram IP o tym adresie zostanie odczytany i przetworzony przez wszystkie komputery danej sieci. Adres sieci i broadcast zmieniają się w zależności od aktualnej przestrzeni adresowej.

Ponadto **adresem specjalnego przeznaczenia** jest adres: 0.0.0.0. oznacza on wszystkie komputery w Internecie. Często podczas odczytywania tablicy rutingu zastępowany jest on słowem: „default”.

Następnym adresem specjalnym jest 127.0.0.1, jest to **adres pętli** (loop-back address). Adres ten służy do komunikacji z wykorzystaniem protokołu IP z lokalnym komputerem (localhost). Jest to adres zawsze przypisany komputerowi, na którym właśnie pracujemy, ponieważ pakiety z takimi adresami nie powinny wydostawać się na zewnątrz komputera, nie powoduje to żadnych konfliktów.

Pewna grupa adresów została zarezerwowana do powszechnego wykorzystania. Można z wykorzystaniem tych adresów budować lokalne intranety (sieci IP świadczące takie same usługi jak Internet, ale dla pojedynczego przedsiębiorstwa). Adresy te czasem nazywane są adresami **nierutowalnymi**. Nazwa ta powstała, ponieważ pakiety z takich sieci nie powinny być przekazywane przez rutery. Wynika stąd, że możemy założyć sobie sieć przestrzenią adresową z takiego zakresu i sieć ta nie będzie widziana na zewnątrz w Internecie. Poniżej przedstawiono zarezerwowane zakresy adresów IP

A 255.0.0.0 10. 0.0.0 - 10.255.255.255
B 255.255.0.0 172. 16.0.0 - 172. 31.255.255
C 255.255.255.0 192.168.0.0 - 192.168.255.255

5.2. Protokół ICMP.

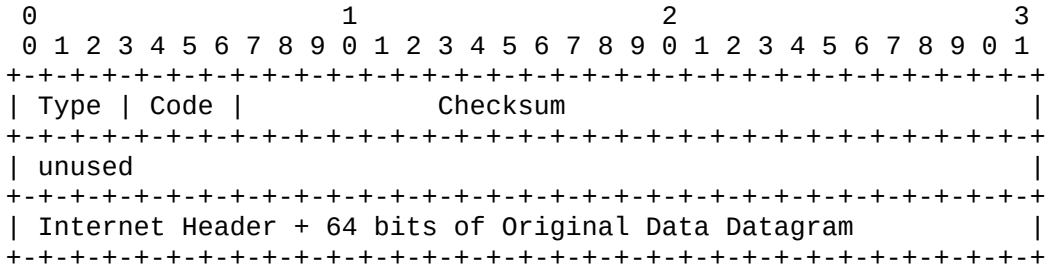
Protokół ICMP (Internet Control Message Protocol) jest częścią warstwy Internetu, do swojego transportu wykorzystuje datagramy IP. Pełni on następujące funkcje:

1. Sterowanie przepływem danych – w przypadku, gdy komputer docelowy transmisji IP nie nadąża za obróbką przychodzących datagramów IP, ICMP wysyła komunikat Source Quench, po którym nadawca czasowo wstrzymuje transmisję.
2. Wykrywanie nieosiągalnych miejsc przeznaczenia – jeśli komputer docelowy nie odpowiada system, który wykrył problem wysyła do nadawcy komunikat Destination Unreachable. Jeśli komunikat ten jest wysyłany przez ruter, oznacza, że ruter nie może wysyłać pakietów do danego komputera. Może to nastąpić w dwóch przypadkach:
   - adres docelowy IP nie istnieje (np.: komputer docelowy jest wyłączony, ma odłączoną sieć, źle ustawioną maskę), występuje wtedy typ komunikatu Host-unreachable,
   - ruter nie może dostarczyć datagramu do tej sieci, występuje wtedy typ Network-unreachable.

   W momencie, gdy komunikat ten jest wysyłany przez host, może to oznaczać, że:
   - dany komputer nie posiada wsparcia dla któregoś z protokołów warstw wyższych, występuje wtedy typ Protocol-unreachable,
   - port protokołu TCP jest nieosiągalny, występuje wtedy typ Port-unreachable.
3. Przekierowywanie ścieżek – jeśli komputer, do którego dotarł datagram IP uzna, że właściwszą bramką będzie inny komputer z tej samej sieci, wysyła komunikat Redirect wskazujący na ten właśnie komputer (musi znajdować się w tej samej sieci). Po otrzymaniu takiego komunikatu nadawca aktualizuje swoją tablicę rutingu.
4. Sprawdzanie zdalnego hosta – odbywa się podczas wywołania komendy ping. Wysyłany jest komunikat Echo Message, po otrzymaniu którego komputer docelowy musi odpowiedzieć. Jeśli tego nie zrobi, uznawany jest za nieosiągalny.
5. Jeśli jakiś datagram, podczas przechodzenia przez ruter osiągnie zerowy limit „czasu życia” (Time-to-Live) jest usuwany. Do komputera źródłowego danego datagramu wysyłany jest komunikat ICMP Time-exceeded.

Protokół ten jest bardzo ważnym protokołem kontrolnym w Internecie. Obsługuje on większość sytuacji awaryjnych i informuje o nich zainteresowane hosty. Bardzo często wykorzystywany jest przy rozwiązywaniu wszelakich typów problemów przez używanie popularnych komend ping i traceroute (w systemach Windows komenda tracert) zaimplementowanych w większości sieciowych systemów operacyjnych.

Format komunikatu Destination Unreachable Message:



Rys. 10. Datagram ICMP

Dany datagram ICMP jest wysyłany wewnątrz datagramu IP na adres docelowy pobrany z orginalnego datagramu.

Pola ICMP:

Type - 3

Code:

0 = net unreachable - sieć nieosiągalna,
1 = host unreachable - host (komputar) nieosiągalny,
2 = protocol unreachable - host docelowy nie obsługuje protokołu warstwy wyższej,
3 = port unreachable - port nieosiągalny,
4 = fragmentation needed and DF set - gdy datagram nie może być sfragmentowany w celu dostarczenia do sieci docelowej,
5 = source route failed - gdy datagram nie może być dostarczony w wyniku problemów z rutingiem lub odłączenia sieci docelowej.

Checksum - Suma kontrolna.

Internet Header + 64 bits of Data Datagram - Nagłówek datagramu na który odpowiadamy oraz 64 bity pola danych.

Podsumowanie typów wiadomości i wartości pola code

0 Echo
0
3 Destination Unreachable
0 = net unreachable;
1 = host unreachable;
2 = protocol unreachable;
3 = port unreachable;
4 = fragmentation needed and DF set;
5 = source route failed.
4 Source Quench
0
5 Redirect
0 = Redirect datagrams for the Network.
1 = Redirect datagrams for the Host.
2 = Redirect datagrams for the Type of Service and Network.
3 = Redirect datagrams for the Type of Service and Host
8 Echo
0
11 Time Exceeded
0 = time to live exceeded in transit;
1 = fragment reassembly time exceeded.
12 Parameter Problem
0 = pointer indicates the error.

13 Timestamp
0
14 Timestamp Reply
0
15 Information Request
0
16 Information Reply
0

5.3. Protokół TCP

TCP (Transmission Control Protocol) realizuje transmisje w trybie połączeniowym. Oznacza to, że między komunikującymi się hostami zestawiane jest wirtualne połączenie. Protokół TCP utrzymuje to połączenie i zapewnia niezawodny transfer danych między hostami. Realizowane jest to poprzez operacje potwierdzania pakietów i retransmitowania pakietów zagubionych. Dokonują tego specjalne algorytmy. W rezultacie program wysyłający dane może mieć pewność ich dostarczenia do odległego hosta.

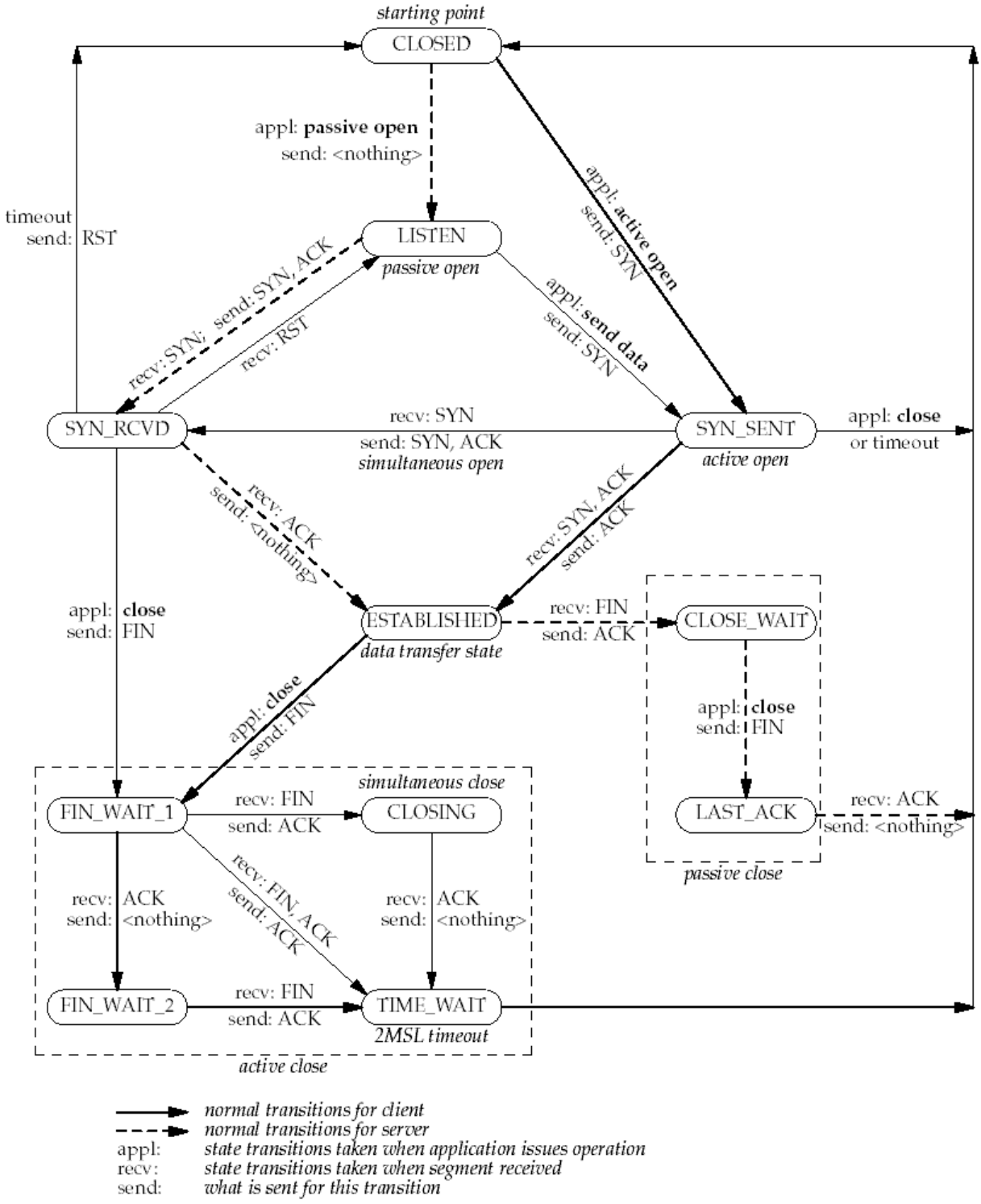
Utworzone połączenie wirtualne zapewnia kanał transmisji, w którym dane przyjmują postać strumienia bajtów. Konkretnie są to dwa strumienie, gdyż transmisja jest dwustronna. Strumień ten nie ma żadnej struktury, nie jest podzielony na żadne rekordy lub inne mniejsze części. Oczywiście przesyłany jest on przy pomocy pakietów (porcji danych) jednak podział strumienia na mniejsze części danych dokonywany przez protokół TCP nie powinien być wiążący dla strony odbierającej. Nadal powinna ona traktować nadchodzące we fragmentach dane jako część strumienia.

Protokół TCP nie zawsze zachowuje podział danych jaki mu sugeruje warstwa zastosowań po stronie wysyłającej. Czasem łączy mniejsze fragmenty, czasem dzieli większe. Przykładowo jeśli program wysyła dwa komunikaty bezpośrednio następujące po sobie, warstwa transportowa może je wysłać w jednym pakiecie. Program odbierający, jeśli zastosuje proste odbieranie danych, może potraktować porcję danych jako jeden komunikat i w rezultacie nastąpi błąd.

Dodatkowo protokół TCP zapewnia obsługę tzw. danych pilnych OOB (ang. urgent data Out-Of-Band). Są to dane przekazywane poza normalnym strumieniem danych, obok niego. Jeśli np. strona wysyłająca wysłała 100 bajtów w normalnym trybie, a odbierająca odebrała dopiero 10 (reszta czeka w buforach wewnętrznych strony odbierającej - tj. zatrzymała się w jednej z warstw), do tego należy się spodziewać, że nieprędko pobierze następne (np. długo przetwarza otrzymane dane) to strona nadająca nie ma możliwości skontaktować się (powiadomić o czymś) strony odbierającej do czasu "przetrawienia" przez nią wszystkich danych.

Wprowadzono możliwość wysyłania komunikatów poza kolejką. Wysłane w tym trybie dane pojawią się na początku danych "nie przetrawionych" przez stronę odbierającą. Tym sposobem następna operacja czytania danych z warstwy transportowej po stronie odbierającej, zwróci dane pilne. W rzeczywistości rzadko się korzysta z możliwości przesyłania danych pilnych, ich zastosowanie komplikuje program i protokół warstwy zastosowań. Należy się wystrzegać stosowania tej możliwości, jeśli dany problem można rozwiązać stosując wyłączenie podstawowy strumień. Spośród popularnych protokołów warstwy zastosowań jedynie TELNET używa danych pilnych i to tylko w wyjątkowych przypadkach.

Podsumowując: Protokół TCP dostarcza niezawodny, połączeniowy, strumieniowy system transmisji danych. Na rys. 10 pokazano graf przejść dla protokołu TCP.



Rys. 10. Graf przejść dla protokołu TCP

Protokół TCP posiada swój nagłówek, którego format pokazano na rys. 11.

<table>
<tr><th>00</th><th>01</th><th>02</th><th>03</th><th>04</th><th>05</th><th>06</th><th>07</th><th>08</th><th>09</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td colspan="16">port źródłowy (nadawcy)</td><td colspan="16">port docelowy (odbiorcy)</td></tr>
<tr><td colspan="32">numer porządkowy</td></tr>
<tr><td colspan="32">numer potwierdzenia</td></tr>
<tr><td colspan="8">dłg.nagłówka</td><td colspan="8">zarezerwowane</td><td colspan="8">bity kontrolne</td><td colspan="8">rozmiar okna</td></tr>
<tr><td colspan="16">suma kontrolna</td><td colspan="16">wskaźnik pilnych danych</td></tr>
<tr><td colspan="32">dane</td></tr>
</table>

Rys. 11. Nagłówek protokołu TCP

Numer wersji – Pierwsze 4 bity nagłówka określają stosowaną wersje protokołu IP, np. 4 lub 6.

Długość nagłówka – Następne 4 bity określają długość nagłówka w krotnościach liczby 32.

Typ obsługi – Seria znaczników określających parametry: pierwszeństwa pakietu (3 bity), opóźnienie (1 bit), przepustowość (1 bit) i niezawodność (1 bit).

Długość całkowita – Długość całkowita pakietu IP w bajtach – maksymalnie 65536.

Niepowtarzalny identyfikator – Liczba 16-bitowa identyfikująca fragment datagramu.

Znacznik fragmentacji – Trzy znaczniki 1-bitowe dotyczące fragmentacji. Pierwszy jest zarezerwowany i zawsze równy 0. Drugi określa dopuszczalność fragmentacji danych pakietów (0 oznacza tak, 1 nie). Trzeci określa pakiet ostatni w serii (0) lub nie (1) – ma znaczenie jeśli drugi znacznik jest równy 0.

Przesunięcie fragmentacji – Przesunięcie sfragmentowanej zawartości względem początku całego pakietu. Wartość mierzona w przyrostach 64-bitowych. Ponowne składanie fragmentowanych segmentów danych jest całkowicie odmienne od ponownego ustawiania w kolejności danych dostarczonych nie po kolei, czym zajmuje się funkcja protokołu TCP.

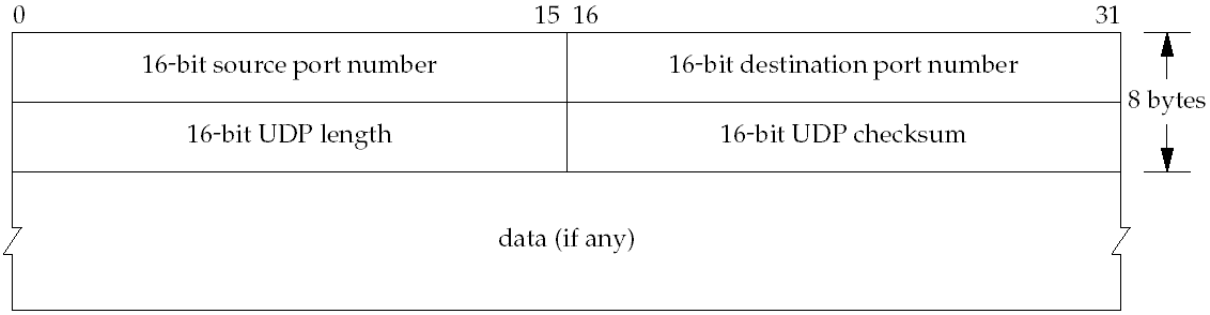
Czas życia (TTL) – Dla każdego przemieszczenia po sieci WAN – skoku wykonanego przez pakiet wartość pola czasu TTL wzrasta o 1. Po osiągnięciu maksimum pakiet uważany jest za *niemożliwy do dostarczenia* (*undeliverable*). Generowany jest i zwracany do komputera źródłowego komunikat protokołu ICMP, a pakiet jest usuwany.

Protokół transportowy – Pole określające protokół warstwy transportowej TCP (wartość 6), UDP (wartość 17) lub komunikat ICMP (wartość 1).

Suma kontrolna – Suma kontrolna nagłówka. Obliczana jest dopełniona do jedynki suma całego nagłówka (z wyzerowanym polem sumy kontrolnej).

5.4. Protokół UDP

Protokół UDP (User Datagram Protocol) jest dużo prostszym protokołem od TCP. Korzysta w sposób mniej wyszukany z warstwy IP. - Wysyła dane z warstwy zastosowań niemalże bez żadnych dodatkowych operacji do warstwy IP. Jedynie dodaje krótki nagłówek m.in. z numerem portu. Można więc powiedzieć, że dane wysłane przy pomocy tego protokołu wędrują więc po sieci jako pakiety IP. Protokół UDP ma więc podobne wady i zalety jak IP. Jest przede wszystkim zawodny - i o tym trzeba zawsze pamiętać. Warstwa zastosowań wysyłając datagram nie ma żadnej pewności, że ten dotrze do adresata i że kolejność odbierania datagramów będzie taka jak nadawania. Musi więc sama zapewniać mechanizmy niezawodności (potwierdzanie, retransmisję itp.).



Rys. 12. Nagłówek protokołu UTP

Zatem zaletą tego protokołu jest to przede wszystkim szybkość. Protokół TCP "traci" dużo czasu na operacje zarządzania połączeniem, potwierdzania danych i retransmisji pakietów utraconych. Czas ten jest niedopuszczalny dla niektórych zastosowań. Niektóre programy korzystają z UDP, zwłaszcza jeśli:

- "zależy im na czasie", czyli stosują protokół czasu rzeczywistego (np. daytime),
- stosują bardzo prosty protokół warstwy zastosowań: jedno pytanie, jedna odpowiedź - wtedy odpowiedź jest jednocześnie potwierdzeniem dostarczenia pytania,
- utrata jednego lub kilku datagramów nie jest rzeczą "tragiczną" (np. w protokołach transmisji głosu będą krótkie przerwy w transmisji),
- z różnych innych względów korzystniej jest skonstruować algorytm zapewniania niezawodności, niż korzystać z protokołu TCP.

Stąd protokół UDP dostarcza zawodnej, bezpołączeniowej usługi przesyłania datagramów.

5.5. Porty

Warstwa transportowa wprowadza pojęcie portów. Port jest dodatkowym polem adresowym, które identyfikuje proces na komputerze odbiorczym. Dzięki temu host "wie" dokąd (do którego programu) ma przekazać dane. Porty są numerowane przy pomocy 16-bitowej liczby dodatniej i w praktyce są częścią (wraz z adresem IP) adresu internetowego. W interfejsach programistycznych istnieje struktura sockaddr_in, która mieści adres IP oraz numer portu. Porty w pamięci zapisuje się w tzw. sieciowym porządku bajtów.

Numery portów pełnią ważną funkcję w zastosowaniach Internetu. Każda standardowa usługa (np. http, POP3, TELNET) ma przypisany ogólnie znany numer portu, który identyfikuje na danym hoście program odpowiedzialny za jej udzielenie. Należy więc pamiętać o tym, aby nowym usługom, stworzonym na potrzeby jednego programu przydzielać numery różne od zarezerwowanych na standardowe usługi. Bezpiecznie jest używać numerów portów większych od 1024.

Przestrzenie adresowe portów dla protokołów TCP i UDP są odrębne. Oznacza to, że można używać jednocześnie jednakowego numeru w stosunku do protokołów TCP i UDP. Nie wchodzą sobie one w drogę.

6. Warstwa zastosowań

Warstwę zastosowań stanowią najczęściej programy użytkownika i programy użytkowe systemu operacyjnego. Korzystają one z warstwy transportowej poprzez interfejs gniazdek. Programy te po obu stronach porozumiewają się ze sobą przy pomocy protokołu warstwy zastosowań. Istnieje wiele standardowych protokołów realizujących różne usługi (HTTP, SMTP, FTP i wiele innych) - wszystkie standardowe protokoły opisane są w dokumentach RFC (Request for Comments). Programy mogą korzystać również z niestandardowych

protokołów, tworzonych do konkretnych zastosowań i konkretnych programów. Wszystkie te protokoły (standardowe i niestandardowe) definiują sposób komunikacji między programami przy zastosowaniu niezawodnego połączenia strumieniowego (TCP) lub zawodnego przesyłania datagramów UTP.

Najważniejsze usługi internetowe:

- Finger – usługa umożliwiająca zdobywanie informacji o użytkowniku mającym konto na zdalnym serwerze. Ze względu jednak na to, że zdobyte w ten sposób dane mogą zostać wykorzystane przez hackerów, obecnie większość maszyn w Internecie ma wyłączoną tą usługę.
- FTP (*File Transfer Protocol*) – protokół transmisji plików umożliwiający obustronną ich transmisję pomiędzy systemem lokalnym i zdalnym.
- Gopher – po polsku „świstak". Obecnie odchodzący w zapomnienie i zastępowany przez WWW, wykorzystywany do wyszukiwania i udostępniania informacji w Internecie dzięki stosowaniu hierarchii menu i plików.
- HTTP (*Hypertext Transfer Protocol*) – protokół przesyłania hipertekstu odpowiedzialny za transmisję stron WWW.
- IRC (*Internet Relay Chat*) – protokół służący do prowadzenia rozmów za pomocą terminala tekstowego.
- NNTP (*Usenet News Transfer Protocol*) – protokół transmisji używany do wymiany wiadomości z serwerami grup dyskusyjnych.
- POP (*Post Office Protocol*) – protokół pocztowy służący do odbioru poczty z serwera i transmisję jej do maszyny lokalnej.
- SMTP (*Simple Mail Transfer Protocol*) – podstawowy protokół transmisji poczty stosowany do wysyłania poczty z maszyny lokalnej na serwer.
- SNMP (*Simple Network Managament Protocol*) – protokół zarządzania siecią. Służy do zdalnej administracji urządzeniami sieciowymi, które udostępniają tą usługę.
- SSH (*Secure Shell*) – bezpieczny protokół terminala sieciowego udostępniający funkcję szyfrowania przesyłanych danych. Jest zalecany do wykorzystania zamiast Telnetu.
- Telnet – protokół terminala sieciowego umożliwiający logowanie się oraz zdalną pracę na odległym komputerze przy wykorzystaniu terminala tekstowego. Cechą charakterystyczną jest transmisja otwartym tekstem, a więc możliwość łatwego podsłuchania tejże transmisji.