

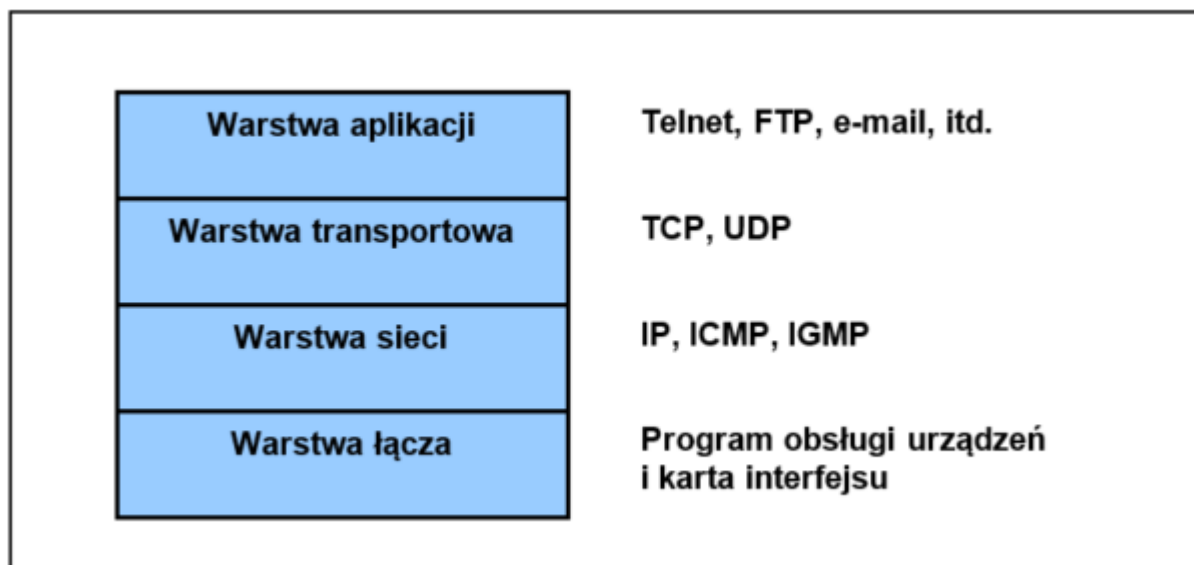
Protokół TCP/IP (część 1)

Zestaw protokołów TCP/IP pozwala na komunikowanie się komputerów różnej mocy obliczeniowej, pochodzących od różnych producentów i pracujących pod kontrolą różnych systemów operacyjnych. Jest to zdumiewające zjawisko, ponieważ wykorzystanie TCP/IP znacznie przekroczyło zakładany na początku zakres zastosowań. To, co pod koniec lat 60 rozpoczęto jako finansowany przez rząd projekt badawczy zmierzający do opracowania sieci pakietowej, w latach 90 zmieniło się w powszechnie używaną formę sieci łączącej miliony komputerów. Jest to naprawdę system otwarty, ponieważ zestaw protokołów i jego kolejne implementacje są w prawie niezmienniej formie powszechnie dostępne w sieci, bezpłatnie lub za niewielką opłatą. Podstawą tego, co powszechnie nazywane jest światowym Internetem lub po prostu Internetem, jest globalna sieć WAN (Wide Area Network), w której pracują miliony komputerów.

Warstwy sieci

Protokoły sieciowe opracowywane są zwykle z uwzględnieniem warstwowego modelu sieci, w którym kolejne warstwy odpowiedzialne są za różne aspekty komunikacji. Zestaw protokołów, taki jak TCP/IP, jest kombinacją różnych protokołów działających w kilku warstwach. Zestaw protokołów TCP/IP rozważa się zwykle jako system czterowarstwowy, jak pokazano na rysunku 2.1. [1].

Rysunek 2.1. Cztery warstwy protokołów TCP/IP



Każda z tych warstw odpowiedzialna jest, za co innego:

Warstwa łącza, nazywana czasami warstwą łącza danych lub warstwą dostępu do sieci, zawiera zwykle programy obsługi urządzeń wchodzące w skład systemu operacyjnego i odpowiadające im karty interfejsów sieciowych w komputerze. Razem tworzą one zestaw obsługujący wszystkie sprzętowe szczegóły związane z fizycznym dołączeniem komputera do kabla sieciowego (lub innych mediów, jakie zostały użyte do budowy sieci komputerowej).

Warstwa sieci nazywana czasami warstwą Internetu obsługuje ruch pakietów w sieci. W tym miejscu następuje na przykład ruting pakietów. W zestawie protokołów TCP/IP warstwę tę tworzą: IP (Internet Protocol), ICMP (Internet Control Message Protocol) i IGMP (Internet Group Management Protocol).

Warstwa transportowa zapewnia przepływ danych pomiędzy dwoma hostami, obsługując znajdującą się nad nią warstwę aplikacji. W skład TCP/IP wchodzić dwa całkowicie różne protokoły warstwy transportowej: TCP (Transmission Control Protocol) i UDP (User Datagram Protocol). Protokół TCP zapewnia niezawodny przepływ danych pomiędzy dwoma hostami. Zajmuje się takimi funkcjami, jak dzielenie danych przekazywanych mu przez aplikacje na kawałki wielkości odpowiadającej warstwie sieci znajdującej się poniżej. Ponadto potwierdza on odebranie pakietów, określa

czasy pozwalające hostowi, z którym następuje wymiana danych, na potwierdzenie ich odbioru i tak dalej. Ponieważ warstwa transportowa zapewnia niezawodny przepływ danych, warstwa aplikacji nie musi już się tym zajmować. Z drugiej strony, protokół UDP umożliwia znacznie prostsze usługi dla warstwy aplikacji. Przesyła między hostami pakiety danych, zwane datagramami, nie gwarantując jednak, że dotrą one do punktu przeznaczenia. W tym przypadku, jeśli żądany jest jakiś poziom niezawodności przesyłania danych, to musi go zapewnić warstwa aplikacji.

Warstwa aplikacji obsługuje funkcje związane z określoną aplikacją korzystającą z sieci. Istnieje wiele aplikacji TCP/IP, które dostępne są w prawie każdej implementacji:

Telnet pozwalający na zdalne zalogowanie się do systemu,

FTP (File Transfer Protocol) protokół transmisji plików,

SMTP (Simple Mail Transfer Protocol) protokół obsługujący pocztę elektroniczną,

SNMP (Simple Network Management Protocol) protokół zarządzania siecią.

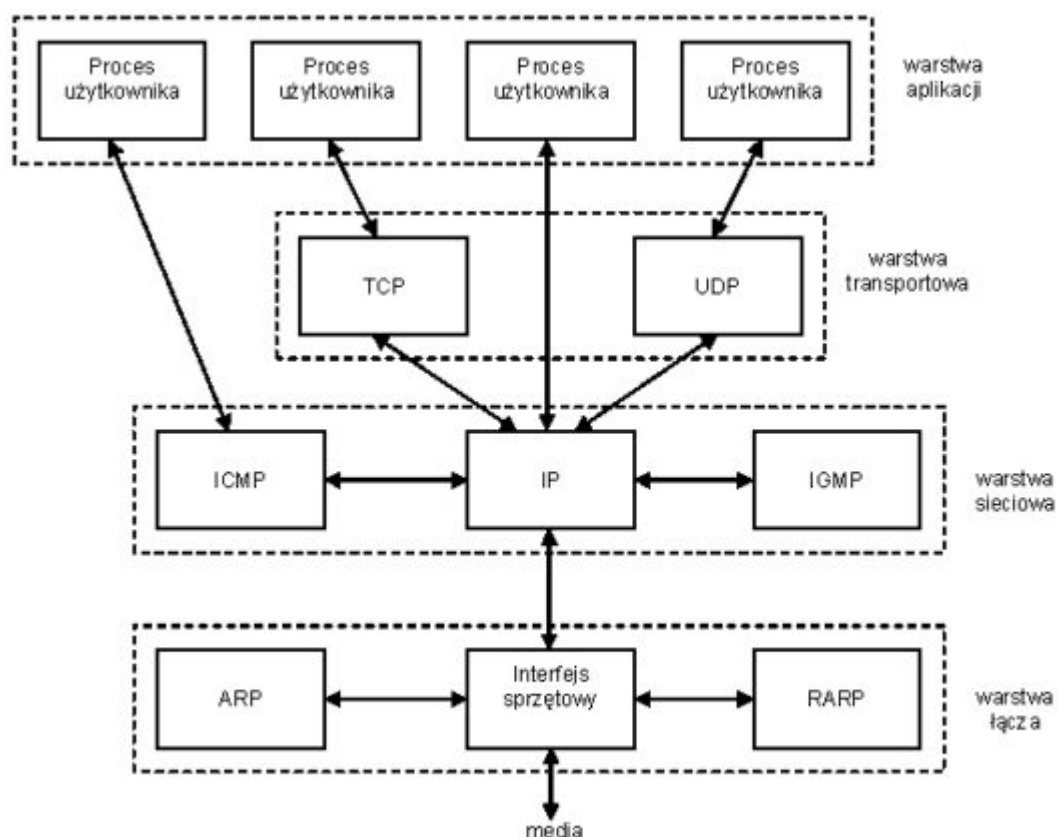
Skład TCP/IP

W zestawie protokołów TCP/IP jest wiele innych protokołów poza tymi, które występują w nazwie. Na rysunku 2.2. przedstawiono kilka innych protokołów wchodzących w skład TCP/IP [1].

TCP (Transmission Control Protocol) i UDP (User Datagram Protocol) są dwoma dominującymi protokołami warstwy transportowej. Obydwa używają IP jako protokołu warstwy sieci. TCP zapewnia niezawodne usługi warstwy transportowej, chociaż posługuje się IP, który nie gwarantuje niezawodności. UDP wysyła i odbiera datagramy przekazywane z aplikacji. Datagram jest jednostką informacji (tzn. określoną przez wysyłającego liczbą bajtów informacji), która przesyłana jest od nadawcy do

odbiorcy. Jednakże w przeciwieństwie do TCP, UDP nie jest usługą niezawodną. Nie ma żadnej gwarancji, że wysłany datagram kiedykolwiek dotrze do celu.

Rysunek 2.2. Różne protokoły wchodzące w skład TCP/IP z podziałem na warstwy, w których pracują



IP jest podstawowym protokołem warstwy sieci. Używany jest on zarówno przez TCP, jak i przez UDP. Każdy segment danych TCP i UDP, który przysyłany jest przez sieć, musi przejść przez warstwę IP zarówno w systemach końcowych, jak i w ruterach pośrednich. Na rysunku 2.2. pokazana jest również aplikacja mająca bezpośredni dostęp do IP. Jest to rozwiązanie możliwe do zrealizowania, choć rzadko stosowane.

ICMP jest protokołem dodatkowym dla IP. Używany jest przez warstwę IP do wymiany komunikatów o błędach i innych ważnych informacji z warstwą IP na innym hoście lub ruterze. Choć ICMP używany jest głównie przez IP, to możliwe jest posługiwanie się nim z poziomu aplikacji (programy diagnostyczne Ping i

Traceroute).

Protokół IGMP (Internet Group Management Protocol) jest używany przy multicastingu: wysyłaniu datagramów UDP do wielu hostów równocześnie.

ARP (Address Resolution Protocol) i RARP (Reverse Address Resolution Protocol) są specjalizowanymi protokołami, używanymi tylko z niektórymi rodzajami interfejsów sieciowych (takimi jak Ethernet i token ring), zapewniającymi konwersję pomiędzy adresami warstwy IP a adresami interfejsu sieciowego.

Protokół IP (Internet Protocol)

IP jest podstawowym protokołem w zestawie TCP/IP. Wszystkie dane z TCP, UDP, ICMP i IGMP przesyłane są przez datagramy IP rysunek 2.3. IP świadczy zawodne, bezpołączeniowe usługi dostarczania pakietów.

Poprzez słowo zawodne (unreliable) rozumiemy to, że nie ma żadnej gwarancji na pomyślne dostarczenie datagramu IP do punktu przeznaczenia. IP stara się jedynie dobrze przesłać datagramy. Kiedy jednak coś się nie uda, na przykład wystąpi przepełnienie buforów routera, IP uruchamia bardzo prosty algorytm obsługi błędów: usuwa datagram i próbuje wysłać do źródła wiadomość ICMP. Wszelkie wymagane mechanizmy niezawodności transmisji muszą być zapewnia ne przez wyższe warstwy (np. TCP).

Określenie bezpołączeniowy oznacza, że IP nie zachowuje żadnej informacji o datagramach, które zostały przesłane pomyślnie. Każdy datagram obsługiwany jest niezależnie od pozostałych. Oznacza to również, że datagramy IP mogą docierać do punktu przeznaczenia w innej kolejności niż zostały wysłane. Jeśli nadawca wysyła dwa kolejne datagramy (najpierw A, potem B) do tego samego punktu przeznaczenia, każdy z nich rutowany jest niezależnie i może być przesłany inną trasą, w wyniku czego B może dotrzeć przed A.

Nagłówek IPv4

Obecnie używaną wersją protokołu jest wersja 4, dlatego czasem IP nazywany jest IPv4. Oficjalną specyfikacją IP jest dokument [4]. Na rysunku 2.3. pokazano format datagramu IP. Typowym rozmiarem nagłówka IP jest 20 bajtów, chyba, że umieszczone są w nim dodatkowe opcje.

Rysunek 2.3. Datagram IPv4 z uwzględnieniem pól tworzących nagłówki IP

4 bity	4 bity	4 bity	4 bity	4 bity	4 bity	4 bity	4 bity
Wersja	Długość	Typ usługi TOS	Całkowita długość pakietu				
Identyfikacja				Znacz-niki	Przesunięcie fragmentacji		
Czas życia (TTL)		Protokół przesyłający dane	Suma kontrolna nagłówka				
Adres źródłowy datagramu – 32 bity							
Adres docelowy datagramu – 32 bity							
Opcje nagłówka (Mogą nie występować)							
Transportowane dane (TCP, UDP ...)							

Przedstawienie cech, możliwości i sposobu działania protokołu IP najłatwiej przedstawić omawiając kolejno znaczenie i zastosowanie poszczególnych elementów struktury danych, jaką stanowi nagłówek protokołu.

Adres źródłowy i docelowy

Wszystkie urządzenia pracujące wewnątrz sieci IP identyfikowane są poprzez unikatowy 32 bitowy adres IP. Wysyłając datagram nadawca umieszcza we właściwych polach adresy IP: swój i odbiorcy oraz dysponując wiedzą z tabeli routingu wysyła datagram do rutera najwłaściwszego z punktu widzenia lokalizacji adresu odbiorcy. W przypadku sieci lokalnej typu ethernet datagram o adresie docelowym IP „lokalnym” dla danej sieci jest wysyłany bezpośrednio do

żądanego komputera, zaś datagramy o innych adresach docelowych są kierowane do rutera – bramki. Zawartość obu pól adresowych nie jest zmieniana w trakcie przesyłania informacji. Sprawia to, że kolejny router wie, kto jest nadawcą informacji oraz gdzie powinna ona dotrzeć, lecz nieznana jest mu dotychczasowa trasa pakietu w sieci (adresy ruterów, które przesyłały datagram). W ten sposób informacja o sposobie dobierania trasy jest silnie rozproszona. Pole adres źródłowy nie odgrywa w procesie dostarczania datagramu istotnej roli, wykorzystywane jest dopiero przez odbiorcę do identyfikowania nadawcy wiadomości.

Czas życia datagramu (TTL)

Ponieważ jak opisano powyżej proces wybierania trasy datagramu zależy w dużej mierze od sprawności działania wszystkich węzłów pośredniczących, możliwe jest, że w sytuacjach awaryjnych pakiet będzie krążył pomiędzy ruterami bardzo długo, lub wręcz trasa jego przesyłania zostanie zapętlona. Pole TTL (Time-To-Live) zapobiega takiej sytuacji – jego zawartość jest wstępnie inicjowana przez nadawcę i dekrementowana przez każdy z węzłów, który przesyła datagram. Gdy jego wartość wyniesie 0, datagram zostaje usunięty, a do nadawcy wysyłany jest komunikat ICMP o błędzie.

Protokół przesyłający dane

Immanentną cechą enkapsulacji danych przez protokoły warstwowe jest fakt, iż najważniejszym zadaniem protokołu warstwy niższej jest dostarczanie danych dla warstwy wyższej. Choć powszechnie używa się akronimu TCP/IP, protokół sieciowy IP, oprócz danych warstwy TCP przenosi również dane protokołu transportowego UDP oraz dane sygnalizacyjne protokołów ICMP i IGMP (które uznane są za element protokołu IP choć stanowią de facto warstwę wyższą). Aby rozróżnić rodzaj przesyłanych w datagramie informacji nadawca umieszcza w tym polu nagłówek liczbę reprezentującą zestandaryzowane oznaczenie protokołu

przesyłanych informacji. Pole to może zostać również użyte przez rutery do traktowania z wyższym priorytetem wiadomości sygnalizacyjnych ICMP.

Suma kontrolna nagłówka

Pole to zabezpiecza integralność informacji przesyłanych tylko w nagłówku datagramu. Z reguły jednak warstwy łącza danych (np. MAC w ethernetie, PPP w połączeniu modemowym) sprawdzają poprawność całej przesyłanej informacji, dodatkowo zaś dane mogą być jeszcze zabezpieczane przed przekłamaniami przez warstwy wyższe.

Identyfikacja

Pole to jest unikalnym numerem, który identyfikuje w sposób jednoznaczny datagram wysyłany z danego hosta. Szesnastobitowa wartość tego pola (65 536 możliwości) w połączeniu z mechanizmem TTL gwarantują, że w danej chwili w sieci nie będą nigdy istniały dwa identyczne pakiety.

Wersja protokołu

Pole to oznacza wprost numer używanego protokołu IP obecnie używana wersja to 4, w przyszłości zastąpi ją IPv6.

Długość nagłówka

Liczba 32-bitowych słów umieszczonych w nagłówku wraz z opcjami tworzy długość nagłówka. Typowa (minimalna) długość nagłówka wynosi 5. Liczba ta informuje komputer odbierający, kiedy ma zakończyć czytanie nagłówka i rozpocząć czytanie danych.

Całkowita długość pakietu

Wielkość ta, pomniejszona o rozmiar nagłówka wyznacza rozmiar pola danych enkapsulowanych przez datagram. Jego teoretyczny rozmiar sięga, co prawda wartości 64kB, jednak w praktyce ze względu na ograniczenia interfejsów fizycznych długość

datagramu nigdy nie przekracza wartości tzw. MTU (*Maximum Transmission Unit*), zaś w wielu przypadkach ze względu na różnice w wielkości największego dopuszczalnego pakietu konieczna jest segmentacja datagramu (podział na kilka pakietów).

Typ usługi TOS

W założeniach, protokół IP posiadać miał pewne elementy mechanizmów sterowania przepływem, których celem jest zapewnienie gradacji poziomu jakości usługi sieciowej (QoS). W tym celu pole TOS zawiera 3 bitowy wskaźnik priorytetu przesyłania pakietu oraz trzy flagi zalecanego doboru trasy, które mogą być używane do określania parametrów pierwszeństwa, opóźnienia, przepustowości i niezawodności tego pakietu. Niestety, obecne implementacje nie używają żadnego z tych pól (tzn. pola te są z reguły ustawiane, lecz elementy komutacyjne sieci – routery ignorują je). Ponieważ transmitowanie informacji przez sieć odbywa się na poziomie sieciowym, utracono w ten sposób możliwość efektywnego i zstandardyzowanego sterowania przepływem na poziomie IP. Istniejące rozwiązania posługują się na ogół informacjami zasięgniętymi z nagłówka TCP w celu rozpoznania rodzaju przesyłanej usługi.

Znaczniki

Pole zawiera 3 bity. Pierwszy jest zawsze zerem. Drugi bit określa czy można (wartość 1), czy też nie można (wartość 0) fragmentować datagram. Natomiast ostatni bit służy do identyfikacji ostatniego fragmentu składającego się na pierwotny datagram. Wartość 0 określa ostatni, a wartość 1 oznacza kolejny fragment.

Przesunięcie fragmentacji

Pole to zawiera 13 bitów, wskazuje, którą częścią całości pierwotnego datagramu jest dany fragment. Poszczególne fragmenty mają pola danych o długości będącej wielokrotnością

8 bitów. Wyjątkiem jest ostatni fragment, którego długość wynika z długości pierwotnego datagramu. W polu tym podaje się o ile zawartość fragmentu jest przesunięta w stosunku do początku pola danych pierwotnego datagramu.

Opcje

To pole nagłówka o zmiennej długości w zamierzeniach autorów umożliwiało uzyskanie między innymi następujących funkcji:

- ograniczenia dotyczące bezpieczeństwa;
- zapisu trasy podróży przez sieć;
- zapisu czasu wyjścia datagramu z danego węzła sieci (router);
- ustalenie swobodnej trasy rutowania – lista węzłów przez które datagram musi przejść (pomiędzy nimi droga może być wybierana dowolnie);
- ustalenie dokładnej trasy rutowania – datagram nie może przejść inną drogą niż wskazaną na liście.

Możliwości pola *opcje* otwierają pewną drogę do wsparcia zastosowań wymagających utrzymywania w miarę stałych i powtarzalnych parametrów opóźnień i przepustowości sieci. W praktyce jednak ze względu na powszechne ignorowanie tej opcji przez rutery oraz zbyt małą dopuszczalną długość tego pola w stosunku do ilości punktów przeskoku na typowej trasie połączenia internetowego, nie można wpływać na sposób przesyłania informacji.

Jeśli szukają Państwo pomocy w napisaniu własnej pracy - potrzebują Państwo fachowych konsultacji to polecamy stronę [pisanie prac](#) - profesjonalna pomoc w pisaniu prac w granicach prawa.