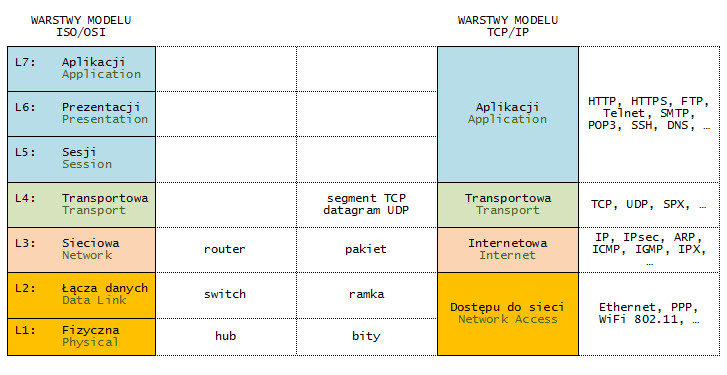
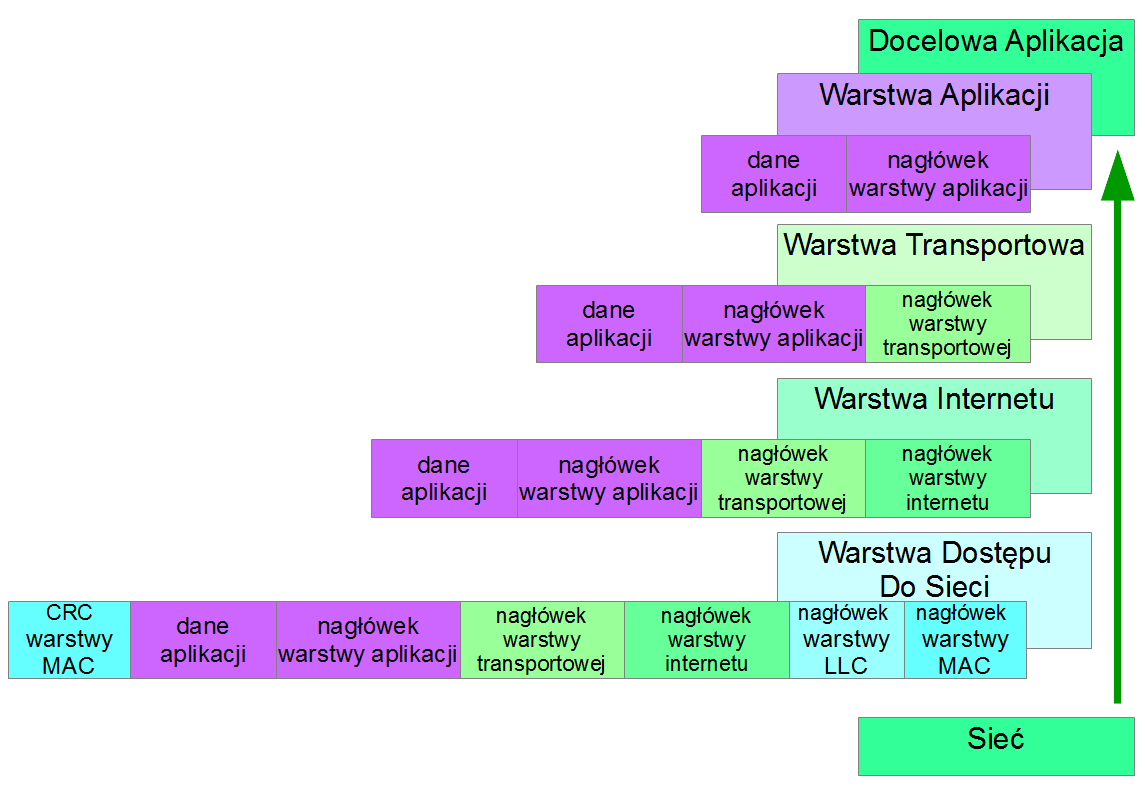
**Protokoły TCP/IP**

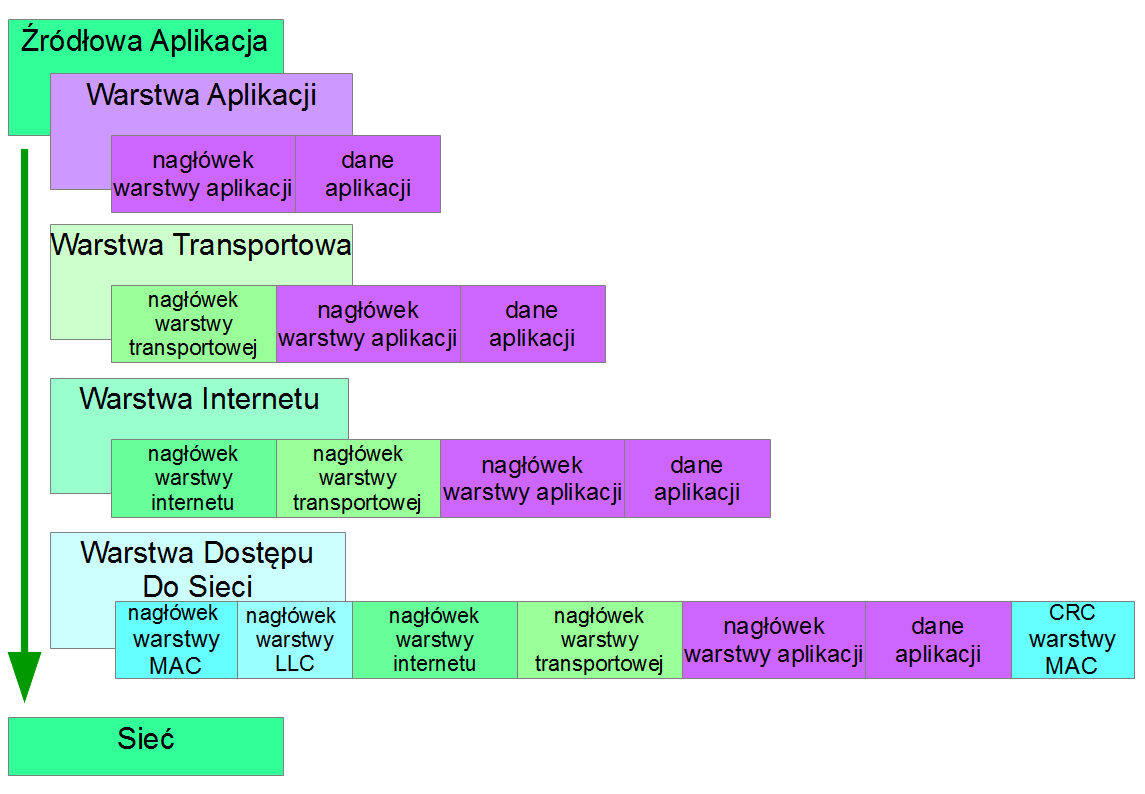
TCP/IP (ang. Transmission Control Protocol/Internet Protocol) to zbiór protokołów służących do transmisji danych przez sieci komputerowe. Model TCP/IP implementuje najważniejsze funkcjonalności siedmiu warstw standardowego modelu OSI.

Poniższy schemat przedstawia odpowiadające sobie warstwy modeli TCP/IP i OSI. 

Każda wiadomość wysłana przez aplikację przechodzi przez wszystkie warstwy TCP/IP, od warstwy aplikacji do najniższej warstwy dostępu do sieci. Następnie jest transmitowana przez sieć do drugiego komputera. Na koniec przechodzi przez wszystkie warstwy w przeciwnym kierunku, aż do warstwy aplikacji i docelowego procesu.

Podczas przesyłania danych z aplikacji do sieci, każda warstwa dodaje swój własny nagłówek (ang. header) do każdej wiadomości. Każdy z tych nagłówków jest potem odczytywany przez odpowiednią warstwę w komputerze odbierającym wiadomość (gdzie wiadomości są przesyłane z sieci do warstwy aplikacji i dalej). Zarówno zawartość jak i wielkość nagłówków zależą od użytych protokołów.

Wysyłanie wiadomości w TCP/IP i jej odbieranie



**Warstwa Aplikacji**

Ta warstwa umożliwia aplikacjom korzystanie z sieci. Istnieje wiele protokołów warstwy aplikacji, które wykorzystują transmisję TCP/IP. Jednymi z ważniejszych protokołów warstwy aplikacji są: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, DNS, IRC, TELNET.

Budowa wiadomości warstwy aplikacji różni się w zależności od protokołu, który został użyty. Niezależnie od formy wiadomości utworzonej przez warstwę aplikacji, warstwa transportowa traktuje każdą otrzymaną wiadomość jako dane i nie wnika w ich zawartość.

**Gniazda sieciowe (ang. internet sockets)**

Każdy proces i aplikacja, kiedy próbuje połączyć się z siecią, muszą powiązać swoje kanały transmisji danych wejściowych i wyjściowych poprzez utworzenie właściwego gniazda sieciowego, które zawiera informacje o adresie IP, numerze portu i użytym protokole warstwy transportowej.

Numer portu może zostać przypisany automatycznie przez system operacyjny, ręcznie przez użytkownika lub może być mu przypisana wartość domyślna, właściwa pewnym popularnym aplikacjom. Numer portu jest 16-bitową liczbą całkowitą (0 - 65535).

Niektóre popularne protokoły warstwy aplikacji używają domyślnych i publicznie znanych numerów porów. Na przykład, HTTP używa portu 80, HTTPS używa portu 443, SMTP portu 25, Telnet portu 23, natomiast FTP używa dwóch portów: 20 do transmisji danych i 21 kontroli transmisji.

Niektóre systemy operacyjne wymagają specjalnych uprawnień do przypisania numerów portów mniejszych niż 1024. Wiele aplikacji preferuje więc używanie portów o wyższych numerach, alokowanych dla nich na krótkie okresy czasu. Takie porty nazywane są portami dynamicznymi

Użytkownik może sprecyzować numer portu w adresie URL. Na przykład, użycie http://www.example.com:8080/path sprawi, że przeglądarka będzie łączyć się ze stroną www przy użyciu portu 8080, zamiast domyślnego portu HTTP, o numerze 80.

Zamknięcie wszystkich portów to 100% bezpieczeństwa komputera i 0% komunikacji i odwrotnie otwarcie wszystkich portów to 100%komunikacji i 0% bezpieczeństwa. Potrzebny jest kompromis – stąd FireWall (zapora sieciowa). Aplikacja śledzi ruch na portach w warstwie sieciowej i reaguje w zależności od ustawień (np. blokada IP, tworzenie dziennika zdarzeń, blokada przekazu itd.)

**Warstwa Transportowa**

Dzieli informację na mniejsze pakiety, dodaje swój własny nagłówek i wysyła wiadomości dalej w dół do warstwy internetowej. Nagłówek zawiera szereg informacji kontrolnych, w szczególności numery portów nadawcy i odbiorcy.

W czasie odbierania danych dzięki numerom portów jest możliwy wybór właściwego protokołu warstwy aplikacji, który powinien otrzymać wiadomość. Przykładowo pakiet, którego docelowy numer portu wynosi 25, będzie dostarczony do protokołu połączonego z tym portem, zwykle SMTP. W tym przypadku, protokół SMTP dostarczy dane do aplikacji email, która ich zażądała.

**TCP**

Najpopularniejszym protokołem warstwy transportowej jest TCP, który zestawia połączenie pomiędzy komunikującymi się stronami przez zainicjowanie tzw. sesji. TCP jest protokołem niezawodnym, w którym odbiorca potwierdza otrzymanie wiadomości. Wszystkie wiadomości dostarczane są w takiej samej kolejności, w jakiej zostały wysłane. TCP jest wykorzystywane w protokołach i aplikacjach, które wymagają wysokiej niezawodności. Nie jest tak szybkie jak UDP, ale -jeśli skonfigurowane poprawnie - TCP zapewnia wciąż dobrą szybkość transmisji połączoną z dobrą jakością przesyłanych danych.

Protokoły warstwy aplikacji, które używane są głównie z TCP to np. HTTP, HTTPS, FTP, SMTP, Telnet.

**UDP**

Drugim popularnym protokołem używanym w warstwie transportowej jest UDP (ang. User Datagram Protocol ). Jest to prostszy protokół, w którym komunikacja odbywa się bez nawiązywania stałego połączenia. Wszystkie pakiety wysyłane są niezależnie od siebie.

UDP jest szybsze niż TCP. Jednak nie zapewnia takiej niezawodności jak TCP, nie gwarantuje, że wiadomości rzeczywiście dotarły do odbiorcy. UDP nie dostarcza pakietów w takiej samej kolejności, w jakiej zostały one wysłane. Ciężar uporządkowania otrzymywanych wiadomości i sprawdzenia czy nie nastąpiły błędy transmisji spoczywa na otrzymującej je aplikacji.

UDP jest preferowane jeśli przesyłane pakiety danych są nieistotne lub komunikacja musi odbywać się z wyjątkowo dużą prędkością. Np. UDP jest używane do przesyłania zapytań DNS (z powodu bardzo dużej liczby zapytań kierowanych do relatywnie niewielu serwerów DNS). UDP jest używane również podczas transmisji audio i video, gdzie utrata pewnej liczby pakietów nie jest bardzo uciążliwa dla odbiorcy.

Protokoły warstwy aplikacji, które używają UDP to np. DNS, DHCP, TFTP, SNMP, RIP, VOIP.

**Warstwa Internetu**

Warstwa internetu dodaje swój nagłówek do wiadomości otrzymywanych z warstwy transportowej. Najważniejszymi polami nowego nagłówka są adresy IP nadawcy i obiorcy. Adres IP jest unikalnym wirtualnym numerem, który umożliwia znajdowanie urządzenia w sieci.

Każde urządzenie sieciowe posiada również inny numer, specjalnie przypisany do niego, nazywany adresem MAC. Jest to unikalny numer, który nie może zostać zmieniony (jest przechowywany w pamięci ROM) i pozwala na jednoznaczne zidentyfikowanie urządzenia na całym świecie. Niestety, zlokalizowanie urządzenia w globalnej sieci na podstawie adresu MAC jest praktycznie niemożliwe, ponieważ numer MAC jest ściśle związany ze sprzętem i producentem urządzenia i nie mówi nic o jego faktycznej fizycznej lokalizacji. Z kolei adres IP pozwala na odnalezienie każdego komputera przy użyciu zapytań do serwerów DNS.

Najogólniej rzecz ujmując, wiadomości sieciowe przechodzą przez wiele routerów zanim osiągną docelowy komputer (wskazywany przez adres IP odbiorcy). Żeby poznać trasę pomiędzy komputerem i docelowym serwerem, można posłużyć się komendą np. tracert www.google.co.uk

Istnieje kilka popularnych protokołów, które działają w warstwie internetowej. Najpopularniejszym i najważniejszym z nich jest IP (Internet Protocol. IP służy do przesyłania pakietów danych przez sieć. Obecnie używane są dwie wersje tego protokołu, IPv4 i IPv6.

IP nie zapewnia żadnego systemu potwierdzania dostarczenia wiadomości, co oznacza, że nie jest niezawodnym (ang. reliable) protokołem. Obowiązek upewniania się, że wszystkie dane zostały dostarczone spoczywa na protokole TCP operującym w warstwie transportowej. Całe połączenie TCP/IP jest więc niezawodne.

**Warstwa Dostępu do sieci**

Warstwa dostępu do sieci umożliwia przesłanie datagramów z warstwy internetowej, przez fizyczną sieć do drugiego komputera, gdzie są one przesyłane przez odpowiadającą jej warstwę dostępu do sieci do warstwy internetowej, a następnie poprzez pozostałe warstwy do docelowej aplikacji. Obecnie, większość komputerów jest podłączona do sieci ethernetowych, które mogą być zarówno przewodowe jak i bezprzewodowe. Wobec tego protokoły TCP/IP wyższych warstw najczęściej są używane razem z zestawem protokołów ethernetowych.

Istnieją trzy warstwy ethernetowe. Pierwsze dwie, Logic Link Control (LLC) i Media Access Control (MAC), odpowiadają warstwie łącza danych w modelu OSI. Trzecia, najniższa warstwa to warstwa fizyczna, podobnie jak w modelu OSI.