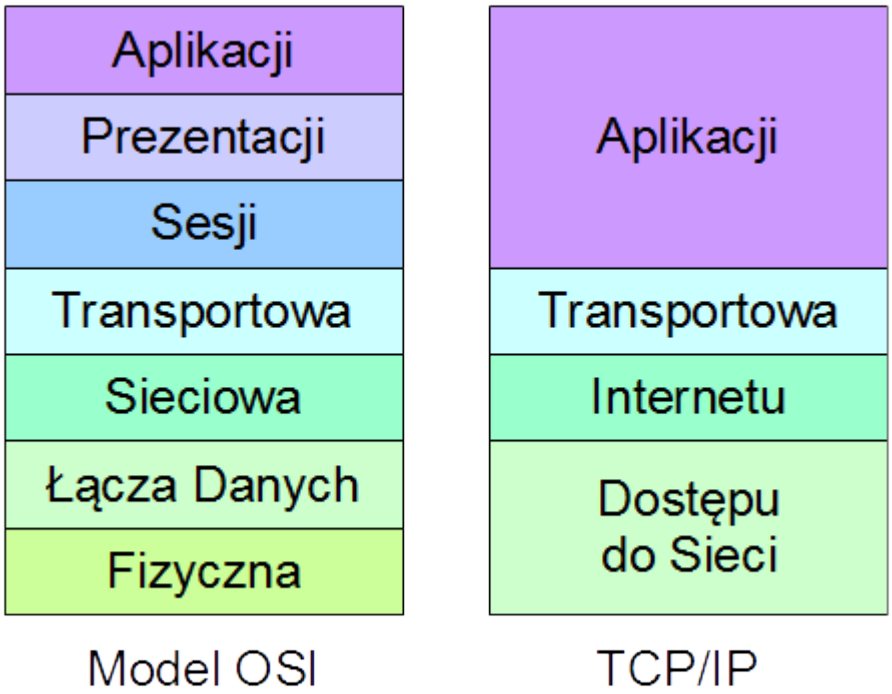
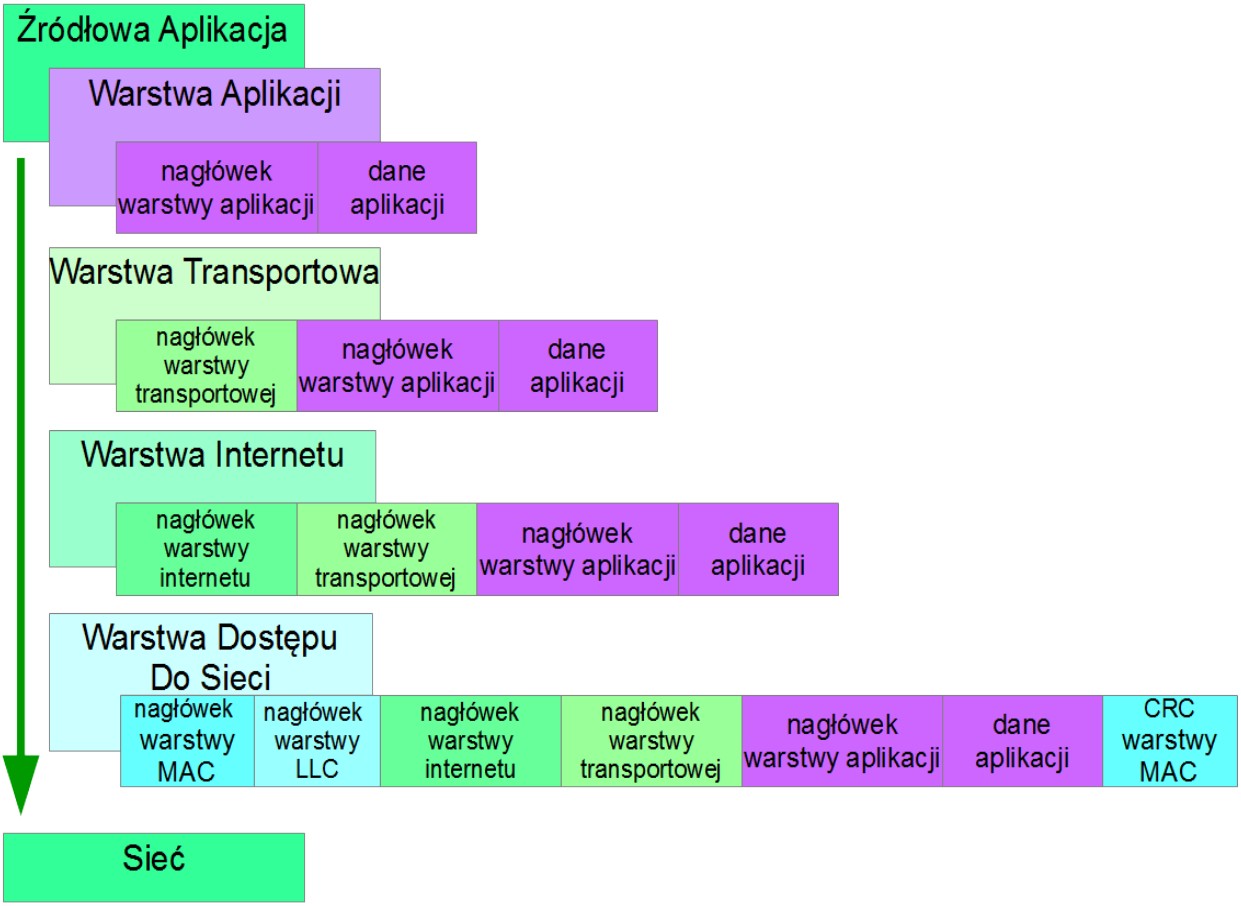
Protokoły TCP/IP

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.

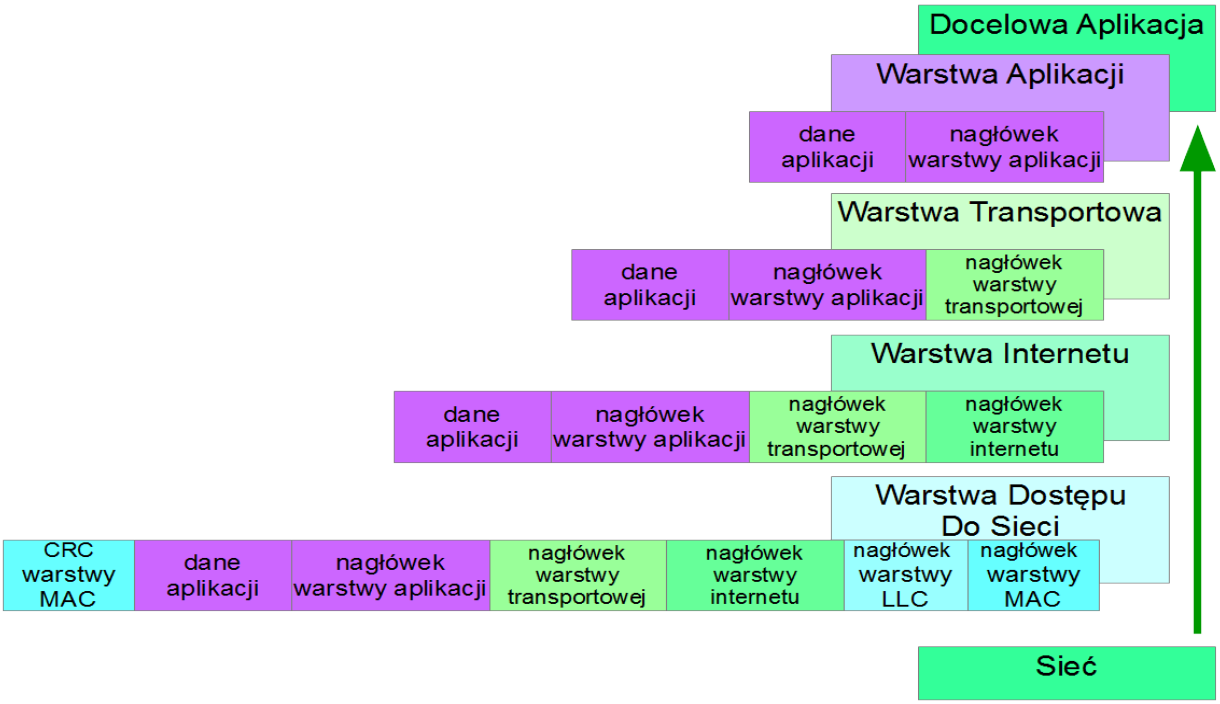


Każda wiadomość wysłana przez aplikację przechodzi przez wszystkie warstwy TCP/IP, od warstwy aplikacji do najniższej warstwy dostępu do sieci. Następnie jest transmitowana przez sieć do drugiego komputera. Na koniec przechodzi przez wszystkie warstwy w przeciwnym kierunku, aż do warstwy aplikacji i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



Odbieranie wiadomości w TCP/IP



Warstwa Aplikacji

Pierwsza z czterech warstw TCP/IP pośredniczy w komunikacji pomiędzy programami komputerowymi i protokołami niższych warstw, umożliwiając w ten sposób aplikacjom

korzystanie z sieci. Programy mogą wykorzystywać różne protokoły warstwy aplikacji do przeprowadzania różnych operacji w sieci.
Istnieje wiele protokołów warstwy aplikacji, które wykorzystują transmisję TCP/IP. Jednymi z ważniejszych protokołów warstwy aplikacji są:
- HTTP, HTTPS - do przeglądania stron www,
- FTP, TFTP, NFS - do transmisji plików,
- SMTP - do wysyłania wiadomości email,
- POP3 - do otrzymywania wiadomości email,
- IMAP - do zarządzania wiadomościami email na serwerach,
- Telnet, rLogin - do zdalnego logowania się na innych komputerach,
- SNMP - do zarządzania sieciami komputerowymi,
- DNS - DNS - do znajdowania adresów IP przypisanych do adresów WWW,
- IRC - do czatów online

Budowa wiadomości warstwy aplikacji różni się w zależności od protokołu, który został użyty. Każdy protokół może wymagać różnych danych wejściowych i produkować różne zapytania, które będą wysłane do warstwy transportowej. 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*)

Gniazda sieciowe to struktury, które są wykorzystywane podczas komunikacji pomiędzy warstwami aplikacji i transportową. Każdy proces i aplikacja, który próbuje połączyć się z siecią, musi powiązać swoje kanały transmisji danych wejściowych i wyjściowych poprzez utworzenie właściwego obiektu gniazda sieciowego.
Obiekt gniazda sieciowego zawiera informacje o adresie IP, numerze portu i użytym protokole warstwy transportowej. Unikalna kombinacja tych trzech parametrów pozwala na zidentyfikowanie właściwego procesu, do którego wiadomość powinna być dostarczona.
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. Lista domyślnych numerów portów jest zarządzana przez organizację Internet Assigned Numbers Authority.
Proces powiązywania aplikacji i gniazda jest nazywany przypisaniem (ang. *binding*). Po zakończonym sukcesem przypisaniu, aplikacja nie musi zajmować się już zarządzaniem siecią, ponieważ wszystkie dalsze operacje leżą w gestii niższych warstw TCP/IP.
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* (ang. *ephemeral ports*).
Użytkownik może sprecyzować numer portu w adresie URL. Na przykład, użycie poniższego URL sprawi, że przeglądarka będzie łączyć się ze stroną www przy użyciu portu 8080, zamiast domyślnego portu HTTP, o numerze 80:

```
http://www.example.com:8080/path
```

Warstwa Transportowa

Warstwa transportowa otrzymuje wiadomości z warstwy aplikacji. Dzieli je 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.
Numery portów są wykorzystywane przez warstwę transportową w czasie obsługiwania pakietów przychodzących z warstwy internetowej (czyli w czasie odbierania danych). Dzięki numerom portów jest możliwe określenie typu zawartości, który znajduje się w przychodzącej wiadomości. Na tej podstawie można wybrać właściwy protokół 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 (ang. *Transmission Control Protocol*). Podczas transmisji danych, TCP zestawia połączenie pomiędzy komunikującymi się stronami (ang. *connection oriented*) przez zainicjowanie tzw. sesji (ang. *session*). TCP jest protokołem niezawodnym (ang. *reliable*), w którym odbiorca potwierdza otrzymanie każdej wiadomości (ang. *acknowledge*). Wszystkie wiadomości dostarczane są w takiej samej kolejności, w jakiej zostały wysłane (ang. *ordering*).
Wszystkie cechy wymienione powyżej są zapewniane prze warstwę TCP. Oznacza to, że TCP może współdziałać z innymi, bardziej zawodnymi protokołami niższych warstw i nie powinno to afektować komunikacji z perspektywy warstwy aplikacji.

Niezawodność TCP

(ANG. RELIABILITY)

W czasie wysyłanie danych, TCP zapewnia, że wszystkie wiadomości zostały dostarczone do miejsca przeznaczenia. Odbiorca testuje każdy otrzymany pakiet pod kątem błędów transmisji (poprzez wyliczanie sumy kontrolnej danych). Jeśli wiadomość jest poprawna, odbiorca wysyła potwierdzenie (ang. *acknowledgement*) do nadawcy. Jeśli nadawca nie otrzyma potwierdzenia w przeciągu określonego (konfigurowalnego) czasu, to ponownie wysyła zagubiony pakiet.
Po kilku nieudanych próbach, TCP zakłada, że odbiorca jest nieosiągalny i informuje warstwę aplikacji, że transmisja zakończyła się niepowodzeniem.

Uszeregowanie pakietów w TCP

(ANG. ORDERING)

Jedno z pól nagłówka TCP zawiera numer sekwencyjny wiadomości. Numer sekwencyjny jest zwiększany o jeden dla każdej wysłanej wiadomości. Podczas odbierania wiadomości, TCP układa pakiety we właściwej kolejności. Dzięki temu, warstwa aplikacji nie musi w ogóle zajmować się kolejnością przychodzących pakietów sieciowych.

Nagłówek TCP

Nagłówek TCP składa się z 20 lub więcej bajtów. Dokładna wielkość zależy od tego czy opcjonalne pole *opcji* (ang. *options*) jest używane. Maksymalna wielkość tego pola to 40 bajtów, więc maksymalna wielkość całego nagłówka to 60 bajtów.

<table>
<tr><th></th><th colspan="4">bity: 0-7</th><th colspan="4">bity: 8-15</th><th colspan="4">bity: 16-23</th><th colspan="4">bity: 24-31</th></tr>
<tr><td>oktety: 0 - 3</td><td colspan="8">port nadawcy</td><td colspan="8">port odbiorcy</td></tr>
<tr><td>oktety: 4 - 7</td><td colspan="16">numer sekwencyjny</td></tr>
<tr><td>oktety: 8 - 11</td><td colspan="16">numer potwierdzenia</td></tr>
<tr><td>oktety: 12 - 15</td><td colspan="4">długość nagłówka</td><td colspan="3">000</td><td>NS</td><td>CWR</td><td>ECE</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="8">szerokość okna</td></tr>
<tr><td>oktety: 16 - 19</td><td colspan="8">suma kontrolna</td><td colspan="8">wskaźnik priorytetu</td></tr>
<tr><td>oktety: 20 - ...</td><td colspan="16">opcje</td></tr>
</table>

Struktura nagłówka TCP

Sesja TCP

W celu wymiany danych przy pomocy TCP, dwie aplikacje muszą najpierw zainicjować sesję (ang. *session*). TCP wymaga wymiany trzech wiadomości żeby utworzyć sesję:

1.**SYN** - pierwsza aplikacja (klient) wysyła pakiet *synchronize* do serwera. Wiadomość zawiera losowy numer sekwencyjny, który został wybrany przez klienta.

2.**SYN-ACK** - serwer odpowiada do klienta. Otrzymany numer sekwencyjny jest zwiększany o jeden i załączany do odpowiedzi jako numer potwierdzenia. Dodatkowo, odpowiedź zawiera inny numer sekwencyjny, losowo wybrany przez serwer.

3.**ACK** - klient potwierdza otrzymanie odpowiedzi od serwera. Wiadomość zawiera oba otrzymane numery zwiększone o jeden.

Kiedy transmisja pomiędzy klientem i serwerem zostanie zakończona, sesja powinna zostać zamknięta. Każda strona komunikacji może zakończyć trwającą sesję. Druga strona powinna odpowiedzieć na to, wysyłając odpowiednie potwierdzenie.

Zastosowanie TCP

TCP jest szeroko 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.

Można wymienić wiele protokołów warstwy aplikacji, które używane są głównie razem z TCP. Jednymi z najpopularniejszych są:

- HTTP, HTTPS
- FTP
- SMTP
- Telnet

UDP

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

Dzięki swojej prostocie UDP jest szybsze niż TCP. Z drugiej jednak strony, nie zapewnia takiej niezawodności działania jak TCP. Przede wszystkim UDP 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.

Nagłówek UPD

Nagłówek UPD składa się z 8 bajtów, jest więc znacznie krótszy niż odpowiadający mu nagłówek TCP.

	bity: 0-15	bity: 16-31
oktety: 0 - 3	port nadawcy	port odbiorcy
oktety: 4 - 7	długość	suma kontrolna

Struktura nagłówka UDP

Zastosowanie UDP

UDP jest preferowane jeśli przesyłane pakiety danych są nieistotne lub komunikacja musi odbywać się z wyjątkowo dużą prędkością. Przykładowo 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.

Istnieje wiele protokołów warstwy aplikacji, które używają UDP, na przykład:

- DNS
- DHCP
- TFTP
- SNMP
- RIP
- VOIP

DCCP

Datagram Congestion Control Protocol jest protokołem, który umożliwia aplikacjom kontrolowanie przepływu danych w celu zapobiegania przeciążeniom sieci (ang. *congestion control*) i utrzymywania stabilnych połączeń. DCCP nie zapewnia niezawodnej (ang. *reliable*) komunikacji z zachowaniem kolejności wysyłanych pakietów.

DCCP jest wykorzystywany przez aplikacje, które operują na szybko zmieniających się danych (dane audio i video, gry online, VoIP). W takich sytuacjach często preferuje się użycie nowej porcji dostępnych danych, zamiast proszenia o retransmitowanie starego uszkodzonego pakietu.

RSVP

Resource Reservation Protocol umożliwia zdalne rezerwowanie zasobów przy użyciu sieci komputerowych. Jest używany głównie przez routery i serwery w celu zapewnienia usług o określonej jakości (ang. *quality of service*, QoS) dla klientów.

RSVP jest w stanie rezerwować pasma transmisji dla komunikacji pomiędzy dwoma komputerami oraz pomiędzy jednym serwerem i wieloma klientami. Wymiana wiadomości w ramach RSVP jest inicjowana przez klienta (odbiorcę), który prosi router (serwer) o zarezerwowanie zasobów.

SCTP

Stream Control Transmission Protocol umożliwia przesyłanie wielu strumieni danych spakowanych razem w pojedynczym strumieniu. Podobnie jak TCP, SCTP zapewnia

niezawodną (ang. *reliable*) transmisję z zachowaniem kolejności pakietów i zapobieganiem przeciążeniom (ang. *congestion control*), dodatkowo rozbudowując jego funkcjonalności o umieszczanie pokrewnych strumieni danych w tych samych wiadomościach.
Ogólnie rzecz biorąc SCTP, jest bardzo rozbudowanym protokołem zapewniającym dobrą jakość komunikacji. Niestety, z racji braku wspierania tego protokołu przez najpopularniejsze routery i systemy operacyjne, nie jest on popularny i szerzej używany.

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 Windowsową:

```
tracert www.google.co.uk
```

Istnieje kilka popularnych protokołów, które działają w warstwie internetowej. Najpopularniejszym i najważniejszym z nich jest IP (*Internet Protocol*), ale warto wymienić też inne protokoły warstwy internetowej:

- ARP (Address Resolution Protocol)
- RARP (Reverse Address Resolution Protocol)
- ICMP (Internet Control Message Protocol)

IP

IP służy do przesyłania pakietów danych przez sieć. Obecnie używane są dwie wersje tego protokołu, IPv4 (*IP version 4*) i IPv6 (*IP version 6*).
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. Cale połączenie TCP/IP jest więc niezawodne.

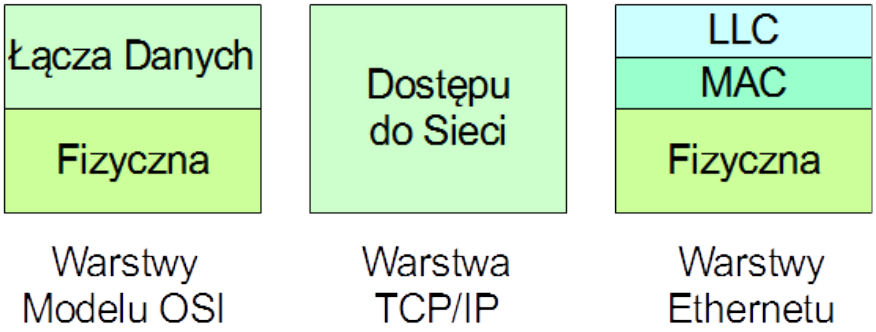
Datagramy IP

Pakiety danych otrzymywane z warstwy transportowej są dzielone na mniejsze datagramy. Każdy datagram zawiera nagłówek IP oraz bajty otrzymane z warstwy transportowej. Maksymalna wielkość datagramu zależy od wersji IP: $216-1$ bajtów dla IPv4 oraz $232-1$ dla IPv6. Jeśli pakiet otrzymany z warstwy transportowej jest zbyt duży, zostanie podzielony na kilka datagramów o odpowiedniej wielkości.
Zwykle dane dzielone są na mniejsze datagramy niż wynikałoby to z ograniczeń protokołu IP. Jest to spowodowane ograniczonymi możliwościami fizycznymi sieci komputerowych. Na przykład, maksymalna wielkość ethernetowych pakietów wynosi 1 500 bajtów, więc zwykle datagramy tworzone w warstwie internetowej operującej na ethernecie będą nieco mniejsze niż 1 500 bajtów (aby umożliwić niższym warstwom

dodanie swoich nagłówków). Maksymalna wielkość datagramu w sieci jest nazywana MTU (*Maximum Transfer Unit*).
IP umożliwia dzielenie datagramów na mniejsze datagramy, jeśli przechodzą one przez sieć z mniejszą wartością MTU. Kiedy mniejsze datagramy docierają znowu do sieci o większej wartości MTU, mogą zostać ponownie zebrane do większego pakietu. W nagłówku IP jest specjalne pole pozwalające na przeprowadzanie takich operacji (nazywające się *Fragment Offset*).

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.



Warstwa Logic Link Control

Najważniejszym zadaniem pierwszej warstwy ethernetu jest przekazanie informacji do docelowej maszyny odnośnie tego jaki protokół powinien być użyty w warstwie transportowej. Umożliwia to poprawne odczytanie przychodzącej wiadomości przez odbiorcę.
Warstwa LLC dopisuje informacje o protokole użytym w warstwie internetowej i o protokole, który powinien otrzymać wiadomość. Pozwala to warstwie LLC na docelowym komputerze poprawnie dostarczyć otrzymane datagramy.
Dokumentację dotyczącą warstwy LLC można znaleźć na stronie IEEE 802.2.

Warstwa Media Access Control

Warstwa MAC jest odpowiedzialna za tworzenie końcowej wiadomości ethernetowej (*Ethernet frame*), która będzie wysłana przez sieć komputerową.
Podobnie jak inne warstwy, warstwa MAC tworzy swój własny nagłówek i dodaje go do wiadomości. Nagłówek zawiera adresy MAC nadawcy i odbiorcy, czyli fizyczne adresy dwóch komunikujących się maszyn. Jeśli docelowa maszyna znajduje się za routerem, w innej sieci, to pole adresu odbiorcy będzie miało wartość adresu MAC routera. Adres MAC odbiorcy będzie zmieniony na inny przez router, kiedy będzie on przetwarzał wiadomość.
Warstwa MAC dodaje również 4 kontrolne bajty CRC, które mogą być wykorzystane do naprawienia uszkodzonej wiadomości.
Warstwa MAC dla sieci przewodowych jest zdefiniowana przez standard IEEE 802.3. Sieci bezprzewodowe są zdefiniowane przez IEEE 802.11.

Warstwa Fizyczna

Warstwa fizyczna jest odpowiedzialna za przekształcanie wiadomości w (zależności od typu sieci) impulsy elektryczne lub fale elektromagnetyczne oraz za transmitowanie ich przez sieć fizyczna pomiędzy komunikującymi się maszynami.
Jest zdefiniowana przez te same specyfikacje co warstwa MAC, IEEE 802.3 i IEEE 802.11.