# Warstwy OSI

**Położenie: (nie dotyczy).**



## Opis

Model **OSI RM** (*Open System Interconnection Reference Model*) został utworzony, aby bezproblemowo przesyłać dane z jednej aplikacji do innej aplikacji znajdującej się na innym komputerze. Zatwierdzony przez ISO w 1984 roku. Bez warstw trzeba by opracowywać osobne protokoły do każdego medium (kabla, światłowodu, radia). Kolejność wysyłania pakietów przez komputer wysyłający:

7. **Warstwa aplikacji** (*application layer,* warstwa **aplikacji** w modelu TCP/IP), np.
- przeglądarka internetowa, interface do połączenia z siecią;
- klient poczty (tworzymy wiadomość);
- protokoły:
  - **DNS** (rekordy: A - autorytatywny adres urządzenia końcowego, drugi poziom, przechowuje informacje o domenach example.com; NS - autorytatywny serwer nazw; CNAME - *canonical name*; MX - rekord wymiany poczty),
  - **DHCP** (rozgłoszeniowy: klient wysyła *DHCPDISCOVER*, serwer odpowiada *DHCPOFFER*, klient przyjmuje propozycję i odpowiada *DHCPREQUEST;* serwer potwierdza dzierżawę poprzez *DHCPACK* lub odmawia poprzez *DHCPNAK* [*Negative Acknowledgement*]),
  - **HTTP**,
  - **P2P**,
  - **POP3**,
  - **SMTP**,
  - **SNMP**,
  - **IMAP**,
  - **telnet**,
  - **FTP** (połączenie sterujące, połączenie danych),
  - **TFTP**.

6. **Warstwa prezentacji** (*presentation layer,* warstwa **aplikacji** w modelu TCP/IP), np.
- wiadomość e-mail zamieniana jest na strumień danych,
- ustawiane są znaki narodowe,
- dane są szyfrowane i kompresowane,
- dane są formatowane do: JPG, GIF, AVI, MP4, MP3, HTML, DOC.

5. **Warstwa sesji** (*session layer,* warstwa **aplikacji** w modelu TCP/IP), np.
- ukierunkowanie strumienia danych (np. e-maila), wznawianie przerwanego dialogu;
- NetBIOS, sockets, SIP, RTP, RPC.

4. **Warstwa transportowa** (*transport layer,* warstwa **transportu** w modelu TCP/IP), np.
- przyjmuje dane z warstwy aplikacji (strumień), komunikuje się z hostem docelowym (poszczególne aplikacje przeprowadzają ze sobą konwersację na unikalnym porcie), aby uzgodnić, jak podzielić dane (np. e-maila) na **segmenty**; nadaje każdemu z nich nagłówek, który określa między innymi kolejność składania tych segmentów przy odbiorze (szeregowanie informacji);
- jeśli nadawca nie otrzyma w określonym czasie potwierdzenia, że wszystkie segmenty dotarły, wysyła utracone segmenty jeszcze raz;
- dane są dzielone na małe segmenty/datagramy, aby wiele aplikacji mogło korzystać z danego łącza w tym samym czasie (multiplikacja) oraz ze względu na ograniczenia sprzętowe (np. rozmiar buforów); możliwe jest ustanawianie wielu sesji równocześnie (np. zakładki w przeglądarce internetowej): porty źródłowe mają wtedy różne losowe numery z zakresu portów zarejestrowanych (klienty), zaś port docelowy ma ten sam numer (np. serwer http:80); kombinacja źródłowego i docelowego IP wraz ze źródłowym i docelowym portem (zazwyczaj w relacji klient-serwer) - zwana jest **gniazdem** (przykładem pary gniazd jest: 192.168.0.1:80 - 192.168.0.6:1099); gniazda umożliwiają przepływ danych z jednej aplikacji do drugiej;
- przeźroczysty transfer danych (między różnymi systemami);

- numery portów określa organizacja IANA (*Internet Assigned Numbers Authority*); dzielą się one na:
    a) dobrze znane porty (0-1023);
    b) porty zarezerwowane dla aplikacji i usług (1024-49151);
    c) porty dynamiczne lub prywatne (49152-65535).
- protokoły:
    a) **TCP** (*Transmission Control Protocol*) - komunikacja połączeniowa (*stateful*; przed wysyłką nawiązuje połączenie z odbiorcą [zestawienie sesji] poprzez wysłanie SYN (*Synchronize Sequence Number*) i odbiór od niego SYN / ACK (A*cknowledgement*, potwierdzenie), w istocie więc są dwie sesje: klient nawiązuje sesję ze serwerem, a serwer nawiązuje sesję z klientem; negocjują parametry połączenia, czyli ilość segmentów w jednostce czasu zależnie od warunków [kontrola przepływu] i sortuje dane), po wysyłce czeka na potwierdzenie odbioru ACK (odpowiednik listu poleconego) oraz zakańcza sesję poprzez wysłanie FIN i otrzymanie potwierdzenia ACK; z protokołu TCP korzysta HTTP, FTP, SMTP, telnet, DNS, SNMP; segment TCP składa się z: port źródłowy, port docelowy, numer sekwencyjny (potrzebny do ponownego złożenia segmentów), numer potwierdzenia, długość nagłówka (*data offset*), zarezerwowane, bity kontrolne (jaką funkcję pełni segment), rozmiar okna (*Window Size*; regulowana dynamicznie ilość segmentów w jednostce czasu; po wysłaniu tej ilości segmentów, nadawca musi otrzymać potwierdzenie ACK od odbiorcy, np. jak odebrał 3000bajtów [rozmiar okna: 3000], to wysyła potwierdzenie o numerze 3001), suma kontrolna, wskaźnik pilności (jak ważne są zamieszczone dane), opcje, dane warstwy aplikacji;
    b) **UDP** (*User Datagram Protocol*) - bezpołączeniowość [brak sesji, nie ostrzega odbiorcy, że będzie coś wysyłał], bez potwierdzenia odbioru, wysyła w takiej kolejności, w jakiej otrzymał dane od aplikacji (składaniem tego w odpowiedniej kolejności mogą zajmować się protokoły wyższej warstwy; brak kontroli przepływu; odpowiednik zwykłego listu - korzystają z tego transmisje *audio/video/gry,* VoIP, TFTP (ma własny system kontroli błędów), DHCP, DNS, SNMP, RIP (w przypadku DHCP i DNS - w przypadku utraty danych, ponownie zostanie wysłane żądanie); tworzy nie segmenty, a **datagramy**, które składają się z: port źródłowy, port docelowy, długość, suma kontrolna, dane warstwy aplikacji;
    c) **SCTP**;
    d) **SSL**;
    e) **TLS**.

3. **Warstwa sieci** (*network layer,* warstwa **Internetu** w modelu TCP/IP), np.
- ustanawianie najlepszych tras dotarcia do konkretnego IP (routing, routery), obsługa błędów przesyłu;
- segment poprzedza **nagłówek IPv4** z adresacją logiczną:
    a) wersja protokołu [0100 = IPv4];
    b) długość nagłówka [IHL = *Internet Header Length*];
    c) zróżnicowanie usługi [informacje dla QoS, info o przeciążeniach];
    d) całkowita długość pakietu (20-65535 bajtów);
    e) identyfikacja fragmentów (stosowane tylko w przypadku fragmentacji pakietu, tj. przy zmianie jego długości [MTU]);
    f) flagi (informują, czy pakiet został pofragmentowany);
    g) przesunięcie fragmentu (numeracja porządkowa pofragmentowanych pakietów);
    h) czas życia pakietu, co zapobiega krążeniu pakietu w pętli w nieskończoność [*TTL = Time To Live;* maksymalna liczba skoków, czyli routerów; licznik ustawiony jest na 255]; gdy router odbierze pakiet z TTL=1 i nie jest on skierowany do niego, wygasza go (nie przekazuje dalej);
    i) protokół [określenie nadrzędnego protokołu: TCP, UDP, ICMP];
    j) suma kontrolna nagłówka;
    k) źródłowy IP;
    l) docelowy IP;
- segmenty mogą również być poprzedzone **nagłówkiem IPv6**, który zawiera:
    a) wersja protokołu [0110 = IPv6];
    b) klasa ruchu (QoS oraz zatory ECN);
    c) znacznik strumienia (*Flow Label*; umożliwia wysyłanie pakietów tę samą trasą, aby nie trzeba było je porządkować przy odbiorze; ma znaczenie w usługach czasu rzeczywistego);
    d) długość danych (długość całego pakietu);

e) następny nagłówek [określenie nadrzędnego protokołu: TCP, UDP, ICMP];
f) limit skoków [maksymalna liczba skoków przez routery];
g) źródłowy IP;
h) docelowy IP;

Nagłówki wraz z segmentami pakowane są do tzw. **pakietów IP**, których wielkość określana jest przez MTU pobrane z warstwy łącza danych; pakiety mogą zostać dodatkowo pofragmentowane przez routery, aby dostosować ich wielkość do różnych mediów, przez które będą przechodzić;
- protokoły warstwy: IP, NAT, IPsec, ICMP (zwrotna informacja o błędach, *ping [ECHO_REQUEST]*, *traceroute;* decyduje o zwolnieniu przepływu datagramów, gdy bufor jest przepełniony; informuje routery o krótszych trasach, o niedostępności celu), IGMP, EIGRP (routing *Cisco*), OSPF (routing, *Open Shortest Path First*;).

Uwaga: Sposobem na przetestowanie działania warstwy sieciowej jest: *ping 127.0.0.1*. Jest to zarazem potwierdzenie działania warstwy łącza danych i warstwy fizycznej.

2. **Warstwa łącza danych** (*data link layer,* warstwa **dostępu do sieci** w modelu TCP/IP), np.
- umieszcza pakiety w **ramce Ethernet** (IEEE 802.3, Xerox w 1973; robi to np. *switch*), której minimalny rozmiar wynosi 64 bajty, a maksymalny 1518 bajty (1522 bajty dla tagów VLAN i QoS; długość ramki uzależniona jest od rodzaju medium i zwana jest MTU [*Maximum Transmission Unit*]); ramki mniejsze niż 64 bajty zwane są "*runt frame*" (karłowate) i mogą świadczyć o wystąpieniu kolizji; warstwa nadaje ramkom **nagłówki** z adresem fizycznym (Preambuła 7-bajtowa [informuje odbiorcę, że nadchodzi ramka, synchronizuje taktowanie], znacznik początku ramki, MAC docelowy [czyli najbliższego routera, nawet jeśli ramka przechodzi przez switch posiadający własny MAC] i MAC źródłowy [adres poprzedniego routera, 48-bitowy w systemie szesnastkowym], typ, długość, kontrola), a także przypisuje **stopki** (4-bajtowa suma kontrolna błędów CRC [*Cyclic Redundancy Check*] analizowana przez pole stopki zwane FCS [*Frame Check Sequence*]); ramka przypomina kopertę w tradycyjnej poczcie, ale dostosowaną do danego medium: kabel miedziany, światłowód, sygnał radiowy, PPP; każdy router na drodze sygnału, rozpakowuje kopertę ramki i tworzy własne ramki (z adresem MAC następnego routera na drodze do celu); ethernet działa w oparciu o rywalizację o medium (metoda niedeterministyczna; nasłuchuje czy w kablu jest sygnał, jeśli nie - zaczyna nadawać) i protokół **wykrywania** kolizji CSMA/CD (*Carrier Sense Multiple Access / with Collision Detection;* metoda deterministyczna) w trybie *half-duplex* **-** w przypadku, gdy dwa media zaczną nadawać jednocześnie; w przypadku *full-duplex* - problem kolizji nie występuje, urządzenia mogą nadawać w tym samym czasie (wymagany jest jednak odpowiedni kabel [prosty / krosowany] lub funkcja *Auto-MDIX*); ramki mogą być przekazywane przez switche albo metodą "*store and forward*" (pobierana jest cała ramka do buforu (najlepiej współdzielonego niż przypisanego do jednego portu] i dopiero przekazywana [po sprawdzeniu poprawności CRC]) lub "*cut-through*" (ramka jest przekazywana dalej, gdy tylko jej część - conajmniej adres docelowy - zostanie otrzymana).
- warstwa posiada dwie podwarstwy: **LLC** (*Logical Link Control; IEEE 802.2,* komunikacja z górną warstwą sieci, pobiera od niej np. pakiety IP; nie wie, jakie medium posiada sprzęt; reprezentacją LLC jest np. sterownik do karty sieciowej) oraz **MAC** (*Media Access Control*, steruje dostępem fizycznym do medium, dodaje do ramki ograniczniki (aby odbiorca wiedział, gdzie się zaczyna i gdzie kończy), dodaje do ramki nagłówek i pole końcowe z sumą kontrolną CRC; odbierając, najpierw sprawdza, czy ramka jest do niego skierowana (adres MAC), a następnie sprawdza sumę kontrolną; standard IEEE 802.3 (*FastEthernet*: IEEE 802.3u; *GigabitEthernet*: IEEE 802.3z); reprezentacją MAC jest np. *firmware* karty sieciowej).
- budowa **ramki PPP** (*Point-to-Point Protocol*, łącze szeregowe): flaga, adres rozgłoszeniowy, sterowanie, protokół, dane, FCS; Uwaga: Ramka PPP nie zawiera adresów MAC (ani źródłowego, ani docelowego), bo łącze szeregowe go nie posiada, więc zawsze wysyłana jest rozgłoszeniowo;
- budowa **ramki wlan** (IEEE 802.11): kontrola ramki, czas trwania, docelowy MAC, źródłowy MAC, MAC pośrednika, sekwencja kontrolna, adres nadajnika, dane, FCS; działa w oparciu o protokół **unikania** kolizji (w przypadku wielodostępu), czyli CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), które polega na tym, że urządzenie najpierw ostrzega, że będzie wysyłało dane;
- MAC, VLAN, ATM, Token Ring, Fibre Channel Frame Relay, ARP (*Address Resolution Protocol*, odwzorowanie MAC na IP, zapytania realizowane w sposób rozgłoszeniowy co 2 minuty), CDP (*Cisco Discovery Protocol*; routery wysyłają co pewien czas ogłoszenia o swojej konfiguracji na adresy MAC swoich sąsiadów), sterowniki; w tej warstwie działa WAN.

1. **Warstwa fizyczna** (*physical layer,* warstwa **dostępu do sieci** w modelu TCP/IP), np.
- zamiana bitów na sygnał zero-jedynkowy (elektryczny / magnetyczny / radiowy / świetlny) i transport do odbiorcy,
- karta sieciowa,
- napięcie elektryczne (określone poziomy reprezentują 0 i 1),
- długość fali,
- przesyłanie strumieni bitów (impulsów).
Sposób wysyłania impulsów może być asynchroniczny (nie jest taktowany żadnym czasem) lub synchroniczny (każdy impuls wysyłany jest w odpowiedniej jednostce czasu). Szerokość pasma to ilość informacji wysłanych w jednostce czasu (np. Mb/s). W tej warstwie działa WAN.

Uwaga: Pakiety w komputerze odbierającym, przechodzą od warstwy 7 do 1. W praktyce następuje tzw. enkapsulacja (na wzór matrioszki): do **ramki** ethernet (jest tam MAC nadawcy i odbiorcy) pakowany jest **pakiet** IP (zawiera numery IP nadawcy i odbiorcy), do niego pakowany jest **segment** TCP, do segmentu pakowane są **dane**.

# Komutacja

Podczas połączenia zestawiane jest dedykowane łącze dla nadawcy i odbiorcy (nikt inny z niego nie korzysta). Przeciwieństwem jest transmisja pakietowa: w tym samym czasie na tym samym kanale transmisyjnym przesyłane są pakiety wielu niezwiązanych ze sobą nadawców i odbiorców.

# WAN

Sieć WAN działa w warstwie fizycznej i w warstwie łącza danych. Może korzystać z takich protokołów, jak:

- **ADSL** (asymetryczne odbieranie i wysyłanie; wykorzystuje linię telefoniczną, ale na częstotliwości wyższej niż 25kHz, czyli nie zakłóca głosu);
- **ATM** (komutacja komórek, łącza wirtualne, tylko jedna trasa, która jest określana przy zestawieniu połączenia);
- **SMDS** (komutacja komórek);
- **DSL**;
- **HDLC**;
- **ISDN** (komutacja kanałów);
- **PPP** (komutacja kanałów);
- **Frame Relay** (komutacja pakietów, ramki o zmiennej długości);
- **X.25** (komutacja pakietów, połączenia między DTE a DCE, czyli między jednym punktem a drugim, zalecane dla WAN).

# Przykład działania HTTP

HTTP jest protokołem aplikacji. Jest on pakowany do TCP (protokół transportowy), który go dzieli na części (segmenty) o odpowiednim rozmiarze (MTU) i ustala z klientem prędkość przesyłu. Segmenty są następnie pakowane do pakietów IP (protokół internetowy), który nadaje im adresy źródłowe i docelowe. Następnie pakiety IP pakowane są w ramki (np. ramki ethernet), których "kształt" (cechy) dostosowane są do medium transmisyjnego (kabel miedziany, światłowód, sygnał radiowy). Każdy router na drodze do odbiorcy, odpakowuje ramkę, analizuje adres IP (aby wybrać najlepszą trasę) i zapakowuje pakiet IP ponownie w ramkę, ale swoją własną (dostosowaną do medium). Klient dokonuje ostatecznej dekapsulacji otrzymanych ramek.

# Dodatkowe informacje

Zasady wysyłania i odbierania są kontrolowane czasem (tzw. *Message Timing*):

- *Access Method* - określenie momentu, w którym nadawca może wysłać wiadomość;
- *Flow Control* - ile informacji można wysłać i z jaką szybkością (wysyłający i odbierający muszą to wspólnie ustalić w oparciu o swoje możliwości sprzętowe);
- *Response Timeout* - czas oczekiwania na odpowiedź (jeśli nie nadejdzie w odpowiednim momencie, odbiorca przestaje już jej oczekiwać).

Wysyłanie może odbywać się:

- do jednej maszyny (*unicast*); adres źródłowy zawsze jest typu *unicast*;
- do wielu maszyn (*multicast*), np. wideokonferencje, rozgrywki CS (grupę identyfikuje się po uruchomionych usługach / portach / protokołach);
- do pierwszej napotkanej (*anycast*) - konfigurowane tylko na routerach;
- do wszystkich maszyn (*broadcast*).

Ostatnia aktualizacja: 31 lipca 2022.