MODEL WARSTW

Ryszard Myhan

Modele warstw

- Modele te wykorzystywane są do opisu różnorodnych funkcji realizowanych przez sieć.
- W takim modelu:
  1. Wszystkie aspekty funkcjonowania sieci dzielone są na mniej złożone elementy.
  2. Projektując i realizując swoje produkty, producenci mogą koncentrować się na określonych obszarach ich konstrukcji.

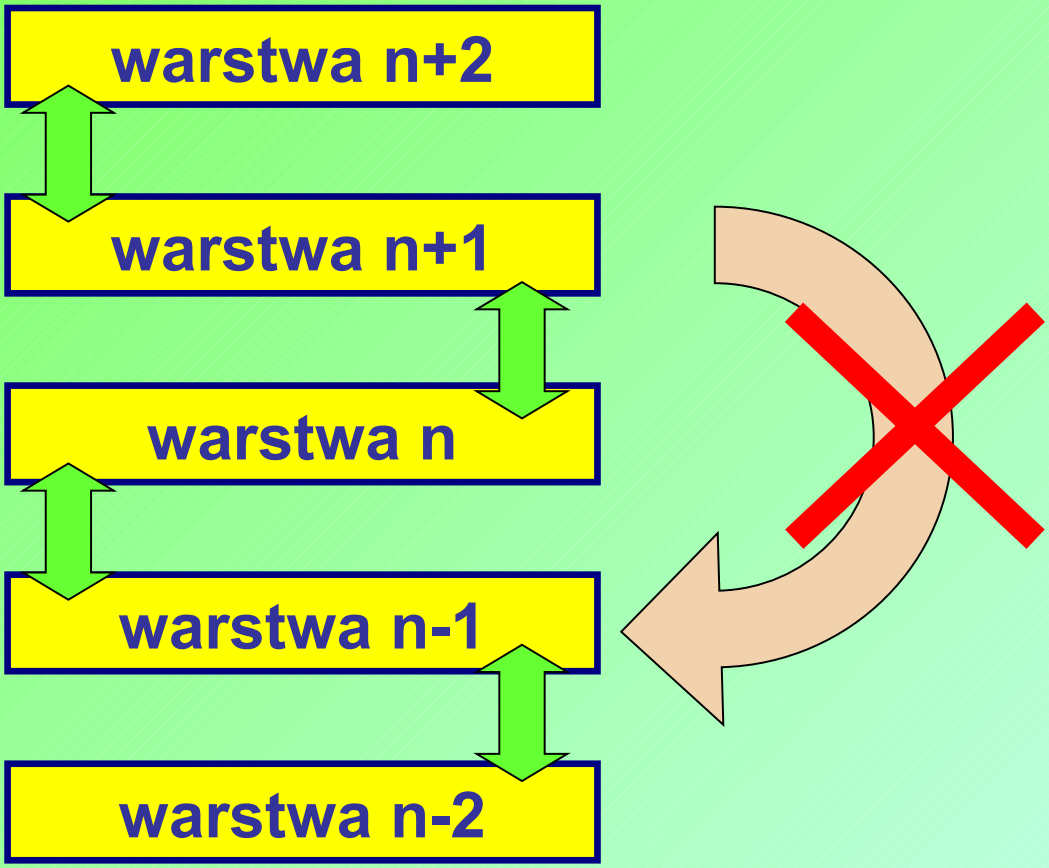
Modele warstw

3. Zmiany w jednej warstwie sieci nie muszą wywoływać zmian w innych (przy założeniu, że warstwa posiada interfejs pośredniczący w komunikacji z pozostałymi).
4. Konstrukcja sieci oparta jest na ściśle określonych podstawach.
5. Model warstwowy pozwala podzielić złożoną pracę sieci na łatwiejsze do zrozumienia i praktycznego opanowania podzbiory działań sieci.

Modele warstw

- Model warstw – założenia:
  1. Każda warstwa powinna być rozważana wyłącznie w powiązaniu z jedną bezpośrednio poniżej i drugą bezpośrednio powyżej.
  2. Z warstwą "*n*" mogą porozumiewać się jedynie warstwa "*n-1*" i warstwa "*n+1*".
  3. Nie jest możliwe aby warstwa "*n*" komunikowała się z warstwą "*n+2*" bez przesyłania danych za pomocą warstwy "*n+1*".

Modele warstw



Model odniesienia OSI

Na początku lat osiemdziesiątych Międzynarodowa Organizacja Normalizacyjna (**ISO** - *International Standards Organization*) dostrzegła potrzebę stworzenia modelu sieciowego, którego zadaniem miało być ułatwienie producentom opracowania współpracujących ze sobą rozwiązań sieciowych.

Model odniesienia OSI

- Powstała wówczas specyfikacja "*Open Systems Interconnection Reference Model*„
- Specyfikacja ta zaadoptowana do polskich norm w 1995 roku jako "*Współdziałanie systemów otwartych - model odniesienia*".

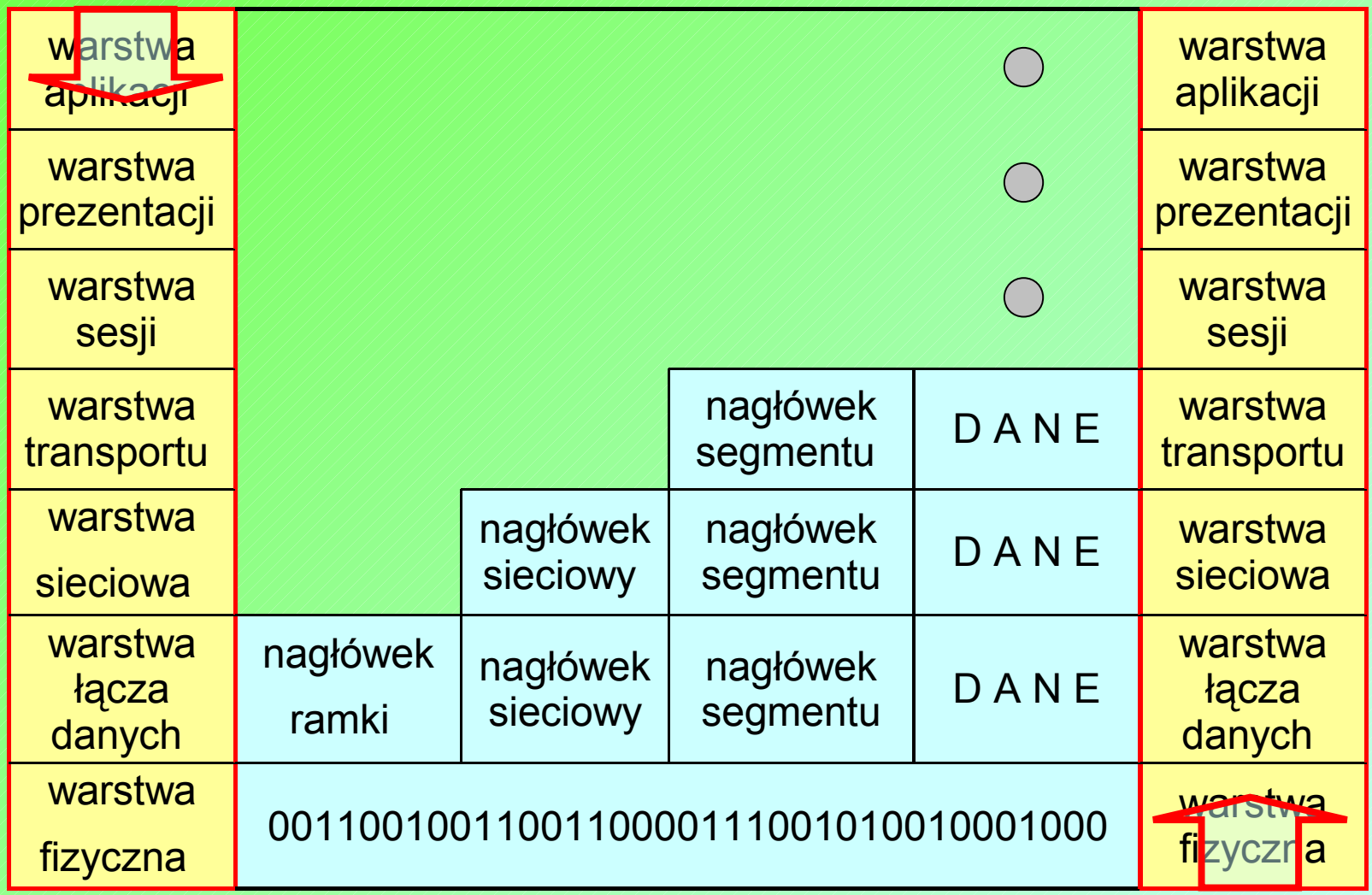
Model odniesienia OSI

- Na wzorzec **OSI** składa się siedem odrębnych warstw:
  1. aplikacji (*application*),
  2. prezentacji danych (*presentation*),
  3. sesji (*session*),
  4. transportu (*transport*),
  5. sieciowa (*network*),
  6. łącza danych (*data link*),
  7. fizyczna (*physical*).

Model odniesienia OSI

- Model ten opisuje drogę danych od aplikacji w systemie jednej stacji roboczej do aplikacji w systemie innej.
- Przed wysłaniem dane zmieniają swój format wraz z przekształcaniem do coraz niższej warstwy sieci.
- W stacji docelowej proces ten przebiega w odwrotnej kolejności.

Model odniesienia OSI



Model odniesienia OSI

WARSTWA FIZYCZNA

- Warstwa fizyczna określa elektryczne lub optyczne parametry wymagane przy przesyłaniu danych między kartą sieciową stacji a systemem komunikacyjnym.
- Warstwa ta obejmuje samo połączenie z systemem komunikacyjnym.
- Dokumentację wymagań i charakterystyki można znaleźć w takich specyfikacjach jak V.35 lub RS-232.

Model odniesienia OSI

WARSTWA ŁĄCZA DANYCH

- Przekazuje ramki danych z warstwy sieciowej do fizycznej i odwrotnie (przy odbiorze).
- Ramka zawiera zazwyczaj następujące elementy:
  - ID odbiorcy (najczęściej adres MAC stacji docelowej lub bramy.
  - ID nadawcy (najczęściej adres MAC stacji źródłowej).
  - Informacje sterujące (dane o typie ramki, trasowaniu, segmentacji itp.).
  - CRC (*Cyclic Redundancy Check*)

Model odniesienia OSI

WARSTWA ŁĄCZA DANYCH

- Warstwa łączy dzieli się na dwie podwarstwy:
  - **Sterowania łączem logicznym** (**LLC** - *logical link control*) - kontroluje poprawność transmisji i współpracuje z warstwą sieciową w obsłudze usług połączeniowych.
  - **Sterowania dostępem do nośnika** (**MAC** - *media access control*) - zapewniającą dostęp do nośnika sieci lokalnej i współpracuje z warstwą fizyczną.

Model odniesienia OSI

WARSTWA SIECIOWA

- Określa najodpowiedniejszą drogę transmisji danych między stacjami.
- Zarządza adresowaniem przesyłek i tłumaczeniem adresów logicznych (jak np. IP) na fizyczne MAC.
- Określa również trasę jaką pokonują dane między stacją źródłową i docelową.
- Zapewnia podział na pakiety.

Model odniesienia OSI

WARSTWA TRANSPORTU

- Segmentuje i składa dane w tzw. strumienie.
- Zapewnia całościowe połączenie między stacją źródłową a docelową.
- Wysyłane dane są dzielone na części, numerowane i wysyłane do stacji docelowej.
- Stacja docelowa, po otrzymaniu danych, wysyła potwierdzenie odbioru.
- Jeżeli pewien segment nie zostanie odebrany, stacja docelowa może zlecić jego ponowne wysłanie.

Model odniesienia OSI

WARSTWA SESJI

- Sesje komunikacyjne zapewniają, że przesyłki są wysyłane i odbierane z zachowaniem wysokiego poziomu niezawodności.
- Warstwa ta realizuje również funkcje ochrony prowadzące do określenia, czy obie stacje mają uprawnienia do komunikowania się przez sieć.

Model odniesienia OSI

WARSTWA SESJI

- Do popularnych protokołów i interfejsów pracujących w warstwie sesji należą:
  - **Winsock** – określa porty, protokoły i adresy obu komunikujących się stacji.
  - **RCP** (*Remote Procedure Calls* – zdalne wywołania procedur) – mechanizm pozwalający przygotować żądanie klienta sieci, aby następnie wykonać je na serwerze przy zachowaniu poziomu zabezpieczeń klienta.

Model odniesienia OSI

WARSTWA SESJI

- Do popularnych protokołów i interfejsów pracujących w warstwie sesji należą:
  - **System X Windows** – pozwalający inteligentnym terminalom na komunikację z komputerami unixowymi w podobny sposób jak przy bezpośrednim połączeniu.

Model odniesienia OSI

WARSTWA PREZENTACJI DANYCH

- W tej warstwie określony zostaje format danych wymienianych między połączonymi komputerami.
- Warstwa prezentacji odpowiada również za wszelkiego rodzaju translacje i szyfrowanie danych, konwersję znaków oraz konwersję protokołów.
- Podstawowe formaty obsługiwane przez nią to:
  - **EBCDIC** (*Extended Binary Coded Decimal Interchange Code*) – rozszerzony kod znakowy.

Model odniesienia OSI

WARSTWA PREZENTACJI DANYCH

- **ASCII** (*American Standard Code for Information Interchnge* – amerykański standardowy kod wymiany informacji) – 8 bitowy zestaw znaków najczęściej stosowanych symboli alfanumerycznych.
- **XDR** (*external data representation*) – zewnętrzna reprezentacja danych) - za jego pośrednictwem realizowane jest przesyłanie tekstu pomiędzy stacjami używającymi różnych reprezentacji znaków.
- Pliki binarne

Model odniesienia OSI

WARSTWA PREZENTACJI DANYCH

- Większość plików dźwiękowych, graficznych i wykonywalnych przekształcana jest w warstwie prezentacji danych do formatu binarnego.
- Przypisanie formatu odbieranych przez stację docelową danych do odpowiedniej aplikacji opiera się wówczas na podstawie rozszerzenia pliku.

Model odniesienia OSI

WARSTWA APLIKACJI

- Za pośrednictwem tej warstwy komunikują się wyłącznie programy korzystające z usług sieciowych.
- Nie kontaktują się z nią programy wymagające jedynie zasobów lokalnych.
- Korzystanie z warstwy aplikacji jest więc uwarunkowane posiadaniem przez program składnika komunikacyjnego, który odwołuje się do zasobów sieci.

Model odniesienia OSI

WARSTWA APLIKACJI

- Przykładowe typy programów wykorzystujących warstwę aplikacji to:
  - Poczta elektroniczna – do najpopularniejszych realizacji należą: Microsoft Exchange Server, Lotus Notes.
  - Elektroniczna wymiana danych (**EDI** – *Electronic Data Interchange*) –usługi realizujące obieg dokumentów, zamówień, dostaw, zapasów i rachunkowości między współpracującymi przedsiębiorstwami.

Model odniesienia OSI

WARSTWA APLIKACJI

- Aplikacje konferencyjne – umożliwiające użytkownikom w oddalonych ośrodkach wymianę obrazu, dźwięku i faksów (np. Microsoft NetMeeting).
- World Wide Web - korzystanie z przeglądarek pozwala użytkownikom z odległych ośrodków na dostęp do danych w różnorodnych formatach – tekstowych, graficznych, dźwiękowych i obrazu wideo.

Model odniesienia OSI

ZALETY MODELU OSI

- ułatwia zrozumienie działania komunikacji sieciowej
- standaryzuje elementy sieci pozwalając na ich rozwijanie przez wielu wytwórców
- pozwala na współdziałanie różnego typu urządzeń sieciowych i oprogramowania
- przeciwdziała wpływowi zmian w jednej warstwie na funkcjonowanie innych warstw
- ułatwia uczenie i uczenie się działania sieci komputerowych

Model warstw TCP/IP

- **TCP/IP** (*Transmisssion Control Protocol / Internet Protocol*) składa się z szeregu protokołów sieciowych.

- Tworzą one zestaw reguł dzięki którym komputery używające różnych systemów operacyjnych są w stanie wymieniać między sobą dane w ustalonym porządku.

Model warstw TCP/IP

1. **TCP/IP** w oparciu o sieć pakietową.
   - Dzięki temu wiele komunikujących się komputerów może przesyłać dane używając tych samych połączeń.
   - Alternatywą jest korzystanie z sieci przełączających, które wymagają dedykowanego obwodu dla każdych dwóch komunikujących się ze sobą urządzeń.

Model warstw TCP/IP

2. **TCP/IP** zapewnia zdecentralizowany nadzór.
   - Każda sieć, która komunikuje się przez TCP/IP otrzymuje zakres numerów do wykorzystania przez komputery tej sieci.
   - Numery te, raz przyznane, pozostają pod nadzorem instytucji, która ich zażądała.
   - Podobnie internetowe nazwy domenowe raz przyznane indywidualnym osobom lub organizacjom mogą być następnie przydzielane lokalnie bez interwencji lub zezwolenia władz wyższego poziomu.

Model warstw TCP/IP

3. W **TCP/IP** komunikujące się urządzenia są partnerami.
   - W odróżnieniu od innych współczesnych sieci, które dzielą komputery na klientów i serwery (NetWare) lub komputery główne i terminale (SNA), TCP/IP uważa wszystkie komputery w sieci za równoważnych partnerów mogących inicjować lub akceptować połączenia.

Model warstw TCP/IP

4. **TCP/IP** wykorzystuje routing.
   - Umieszczone między sieciami routery po prostu przesyłają dane zawarte w odpowiednim polu pakietu sieciowego z jednej sieci do drugiej.
   - W nieroutowalnych protokołach sieciowych trzeba stosować bramy protokołowe, które tłumaczą dane jednej sieci tak, aby odpowiadały one schematowi adresowania i formatowi danych drugiej sieci.

Model warstw TCP/IP

5. **TCP/IP** jest niezależne od konkretnego medium transmisyjnego.
   - Pracuje z Ethernetem, Token ring, ARCnet, FDDI, USB, połączeniami szeregowymi, radiem krótkofalowym (AX.25) i innymi mechanizmami.
6. **TCP/IP** jest standardem otwartym.
   - Wszystkie dokumenty opisujące standard są dostępne w Internecie, można je za darmo ściągnąć i zaimplementować.

Model warstw TCP/IP

7. **TCP/IP** jest odporne.
   - Zostało zaprojektowane gdy, linie telekomunikacyjne nie były w pełni wiarygodne, dlatego protokoły TCP/IP musiały wykrywać i korygować błędy transmisji, przywracać chwilowo zerwane połączenia, a nawet obchodzić uszkodzone części Internetu.

Model warstw TCP/IP

8. **TCP/IP** elastyczne.
   - TCP/IP jest to zestaw protokołów obejmujący protokół IP i kilka innych protokołów warstw niskich oraz protokoły zapewniające coraz bardziej rozbudowane usługi umieszczone w warstwach wysokich.
8. **TCP/IP** pragmatyczne.
   - Wyrosło z prostego zestawu protokołów. Protokoły dodatkowe dodawane były stopniowo w miarę jak implementujący znajdowali więcej zastosowań.

Model warstw TCP/IP

10. TCP/IP nie jest doskonałe.

- Dwoma znaczącymi ograniczeniami jest adresowanie i bezpieczeństwo.
- Protokół był projektowany dla komputerów uniwersyteckich i wojskowych,
- W tych czasach wydawało się, ze 32 bity przestrzeni adresowej (możliwość zaadresowania ok. 4 miliardów komputerów) to dużo.

Model warstw TCP/IP

10. TCP/IP nie jest doskonałe.

- Obecnie jednak do Internetu, oprócz komputerów i routerów przyłączane są też drukarki, serwery terminali, skanery, kamery, faksy i inne urządzenia.
- Ponadto numery przydzielane są w blokach i nie wszystkie są wykorzystywane.

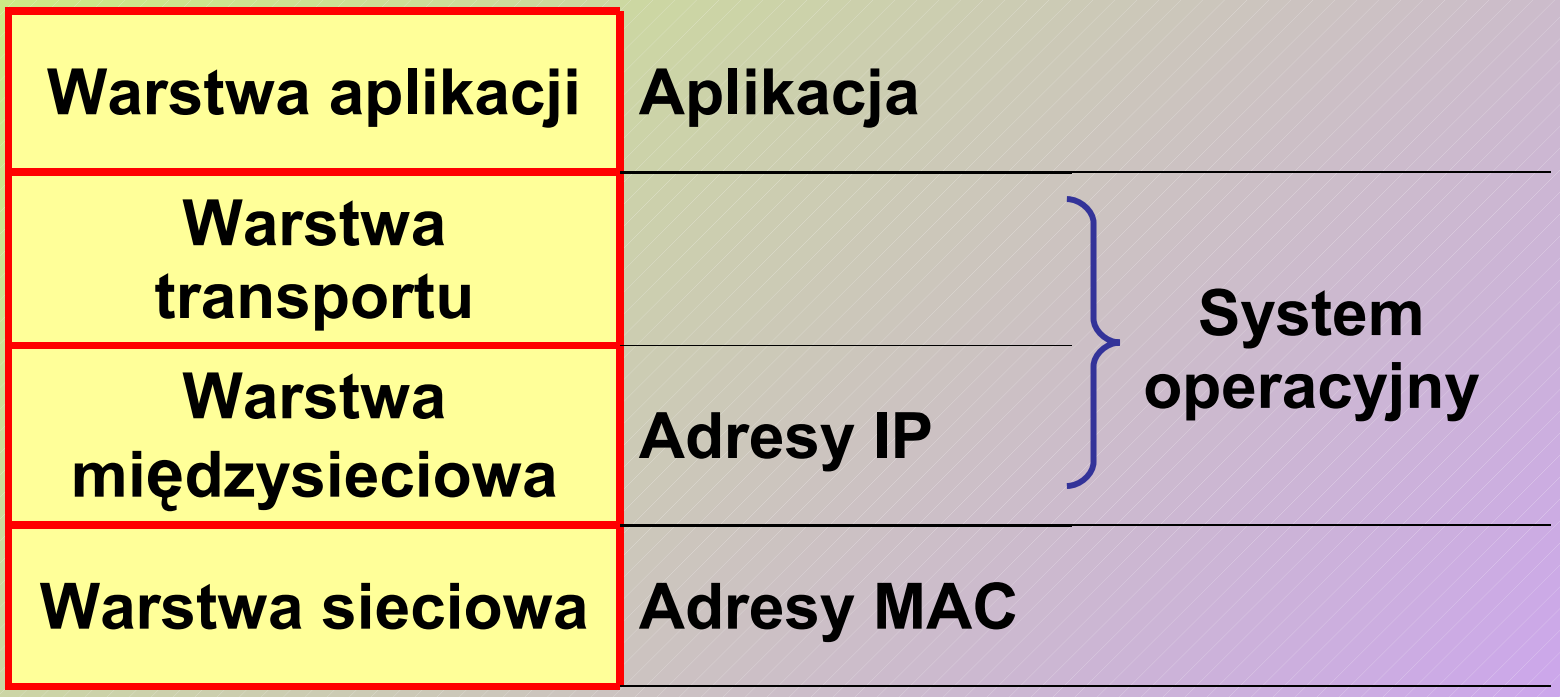
Model warstw TCP/IP

10. TCP/IP nie jest doskonałe.

- Mimo zastosowań wojskowych projektanci TCP/IP nie poświęcali też zbyt dużo czasu na zabezpieczenie TCP/IP przed podsłuchiwaniem danych, przechwytywaniem połączeń, atakami związanymi z uwierzytelnianiem i innymi zagrożeniami sieci.

Model warstw TCP/IP

- Model warstw TCP/IP obejmuje cztery poziomy.



Model warstw TCP/IP

WARSTWA INTERFEJSU SIECIOWEGO

- To najniższy poziom oprogramowania TCP/IP, odpowiedzialny za przyjmowanie datagramów IP i przesyłanie ich poprzez daną sieć;
- Warstwa ta może składać się ze sterownika urządzenia lub ze skomplikowanego podsystemu, który wykorzystuje własny protokół łącza.

Model warstw TCP/IP

WARSTWA INTERFEJSU SIECIOWEGO

- Oprócz umieszczonej na początku ramki preambuły, warstwa sieciowa dodaje również tzw. wartość kontrolną redundacji cyklicznej (**CRC** – *Cyclic Redundary Check*).
- Pozwala ona sprawdzić poprawność przesyłu danych – po dotarciu ramki do punktu docelowego jest obliczana ponownie i porównywana z oryginałem.
- Ramki bez błędów są przekazywane kolejnym warstwom, ramki uszkodzone są odrzucane.

Model warstw TCP/IP

WARSTWA MIEDZYSIECIOWA

- Warstwa międzysieciowa pełni trzy podstawowe funkcje:
  - adresowanie,
  - formatowanie pakietów,
  - trasowanie.
- Warstwa ta odpowiada za obsługę komunikacji jednej maszyny z drugą.

Model warstw TCP/IP

WARSTWA MIEDZYSIECIOWA

- Przyjmuje ona pakiety z warstwy transportowej razem z informacjami identyfikującymi maszynę - odbiorcę, kapsułkuje pakiet w datagramie IP, wypełnia jego nagłówek, sprawdza czy wysłać datagram wprost do odbiorcy czy też do routera i przekazuje datagram do interfejsu sieciowego.
- Warstwa ta zajmuje się także datagramami przychodzącymi, sprawdzając ich poprawność i stwierdzając czy należy je przesłać dalej czy też przetwarzać na miejscu.

Model warstw TCP/IP

WARSTWA MIEDZYSIECIOWA

- W warstwie tej znajduje się protokół IP.
- Nagłówek dodany przez protokół IP do danych zawiera:
  - Źródłowy adres IP (stacji wysyłającej).
  - Docelowy adres IP (stacji przeznaczenia).
  - Informacje jakiego protokołu użyto w warstwie transportu (UDP lub TCP).
  - Sumę kontrolną – pozwalającą wykryć uszkodzenia danych.

Model warstw TCP/IP

WARSTWA MIEDZYSIECIOWA

- Czas życia (TTL - *time-to-live*) – wartość zmniejszana co najmniej o 1 przy każdym przejściu datagramu przez router.

Model warstw TCP/IP

WARSTWA MIEDZYSIECIOWA

- Warstwa ta wyznacza również drogę datagramu do stacji docelowej:
  - Gdy jest ona w tym samym segmencie sieci, datagram wysyłany jest bezpośrednio do miejsca przeznaczenia.
  - Jeżeli stacja docelowa znajduje się w segmencie odległym, za pomocą tabeli tras stacji źródłowej określana jest trasa do sieci tej stacji.

Model warstw TCP/IP

WARSTWA MIEDZYSIECIOWA

- Gdy tabela nie zawiera odpowiedniej trasy, stacja źródłowa wykorzystuje do przesłania datagramu bramę domyślna (router wykorzystywany przez stacje do kierowania ruchu do odległych segmentów sieci).

Model warstw TCP/IP

WARSTWA MIEDZYSIECIOWA

- Do pozostałych procesów realizowanych w warstwie międzysieciowej należą fragmentacja oraz składanie.
- Do każdego z powstałych w procesie fragmentacji pakietów dołączane są następujące informacje:
  - Znacznik – ustawienie bitu znacznika w nagłówku każdego fragmentu pakietu oznacza, że dane zostały poddane fragmentacji; brak ustawionego znacznika oznacza, że jest to ostatni fragment pakietu.

Model warstw TCP/IP

WARSTWA MIEDZYSIECIOWA

- Identyfikator fragmentu – każda część dzielonego datagramu otrzymuje swój ID, który wykorzystywany jest przy jego składaniu u odbiorcy.
- Pozycja fragmentu – umożliwiająca odtworzyć porządek składania.

Model warstw TCP/IP

WARSTWA TRANSPORTU

- Podstawowym zadaniem warstwy jest zapewnienie komunikacji między jednym programem użytkownika a drugim.
- Warstwa ta może regulować przepływ informacji, może też zapewnić pewność przesyłania.
- W tym celu organizuje wysyłanie przez odbiorcę potwierdzenia otrzymania oraz ponowne wysyłanie utraconych pakietów przez nadawcę.

Model warstw TCP/IP

WARSTWA TRANSPORTU

- Wykorzystywane są do tego dwa protokoły transportowe:
  - Protokół Sterowana Transmisją (**TCP** – *Transmission Control Protocol*).
  - Protokół Datagramów Użytkownika (**UDP** – *User Datagram Protocol*).
- O tym który z protokołów zostanie użyty nie decyduje administrator lecz zależy to jedynie od aplikacji wysokiego poziomu.

Model warstw TCP/IP

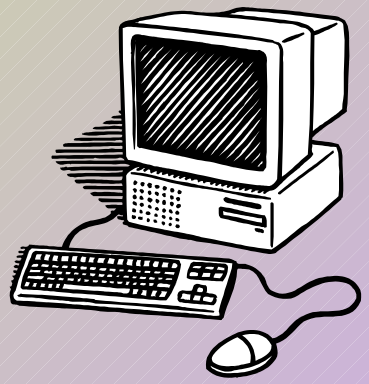
WARSTWA TRANSPORTU

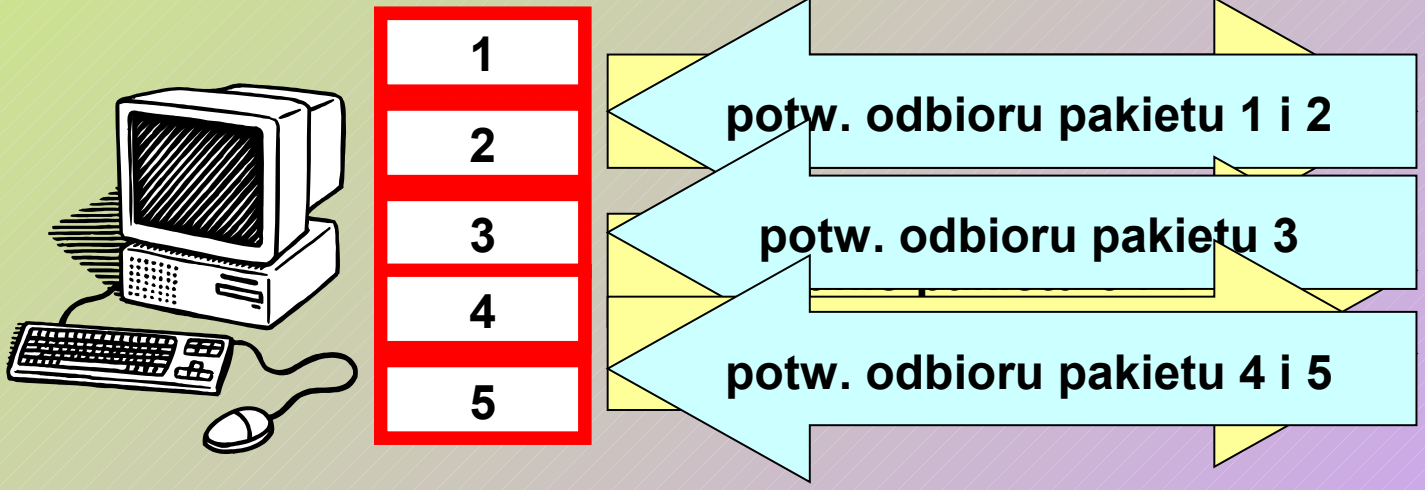
- Aby dwie stacje komunikowały się ze sobą przy użyciu TCP, konieczne jest ustanowienie pomiędzy nimi **sesji**.
- Za pomocą numerów sekwencyjnych i zwrotnego przesyłania potwierdzeń odbioru danych zapewniona jest kontrola nad odbieranymi danymi.
- Jeżeli stacja docelowa nie otrzyma określonego segmentu, może przesłać stacji źródłowej żądanie ponownego przesłania pakietu o odpowiednim numerze sekwencyjnym.

Model warstw TCP/IP

WARSTWA TRANSPORTU

sesja połączeniowa TCP





Model warstw TCP/IP

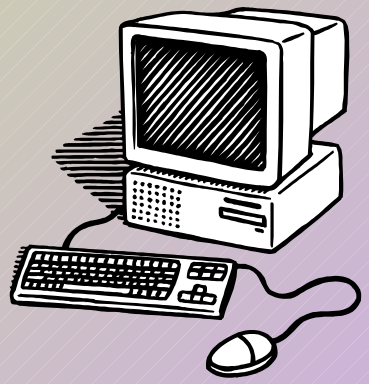
WARSTWA TRANSPORTU

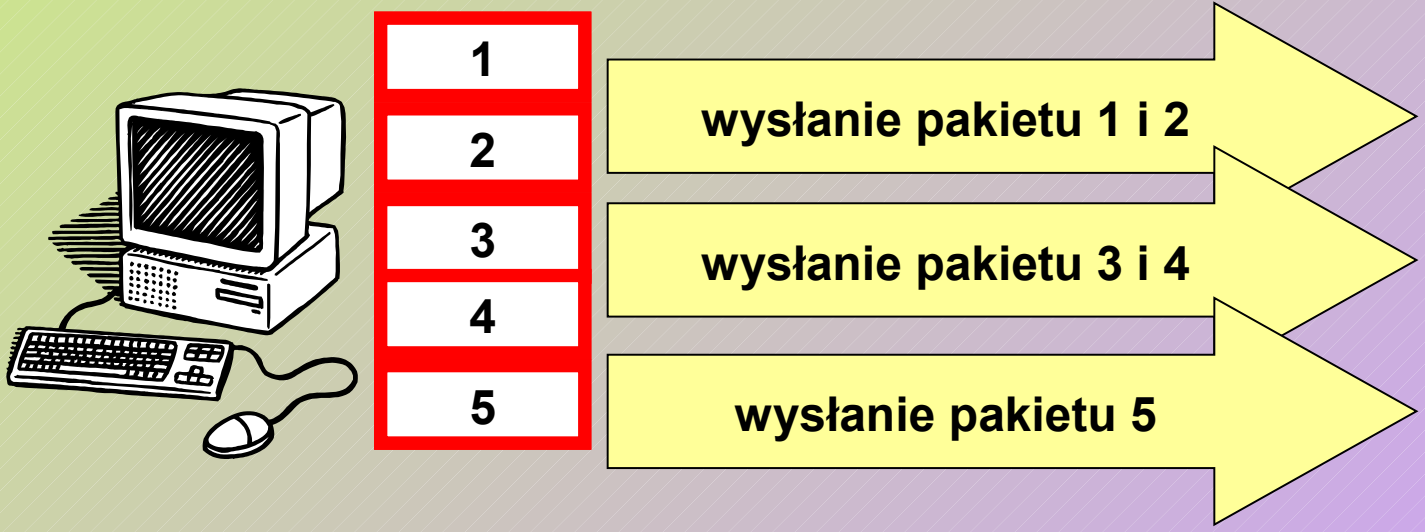
- Protokół **UDP** realizuje usługę bezpołączeniową.
- Nie ma gwarancji, że stacja docelowa otrzymała dane.
- Kontrola nad tym pozostawiona jest wykorzystującym ten protokół aplikacjom.

Model warstw TCP/IP

WARSTWA TRANSPORTU

usługa bezpołączeniowa UDP





Model warstw TCP/IP

WARSTWA APLIKACJI

- Pojęcie „aplikacje sieciowe” oznacza tu aplikacje, które podłączają się do zdalnych stacji sieciowych lub komunikują się za ich pośrednictwem.
- Aplikacje pracujące w sieciach TCP/IP należą do jednej z dwu grup:
  - aplikacje Winsock
    (np. FTP, Telnet, SNMP, IRC)
  - aplikacje NetBIOS
    (np. składniki sieciowe Windows NT 4.0).

Porównanie modeli OSI i TCP/IP

1. Model TCP/IP łączy warstwę fizyczną i łącza danych modelu OSI w jedną warstwę interfejsu sieciowego - pozwala to implementować TCP/IP w dowolnej topologii sieci.

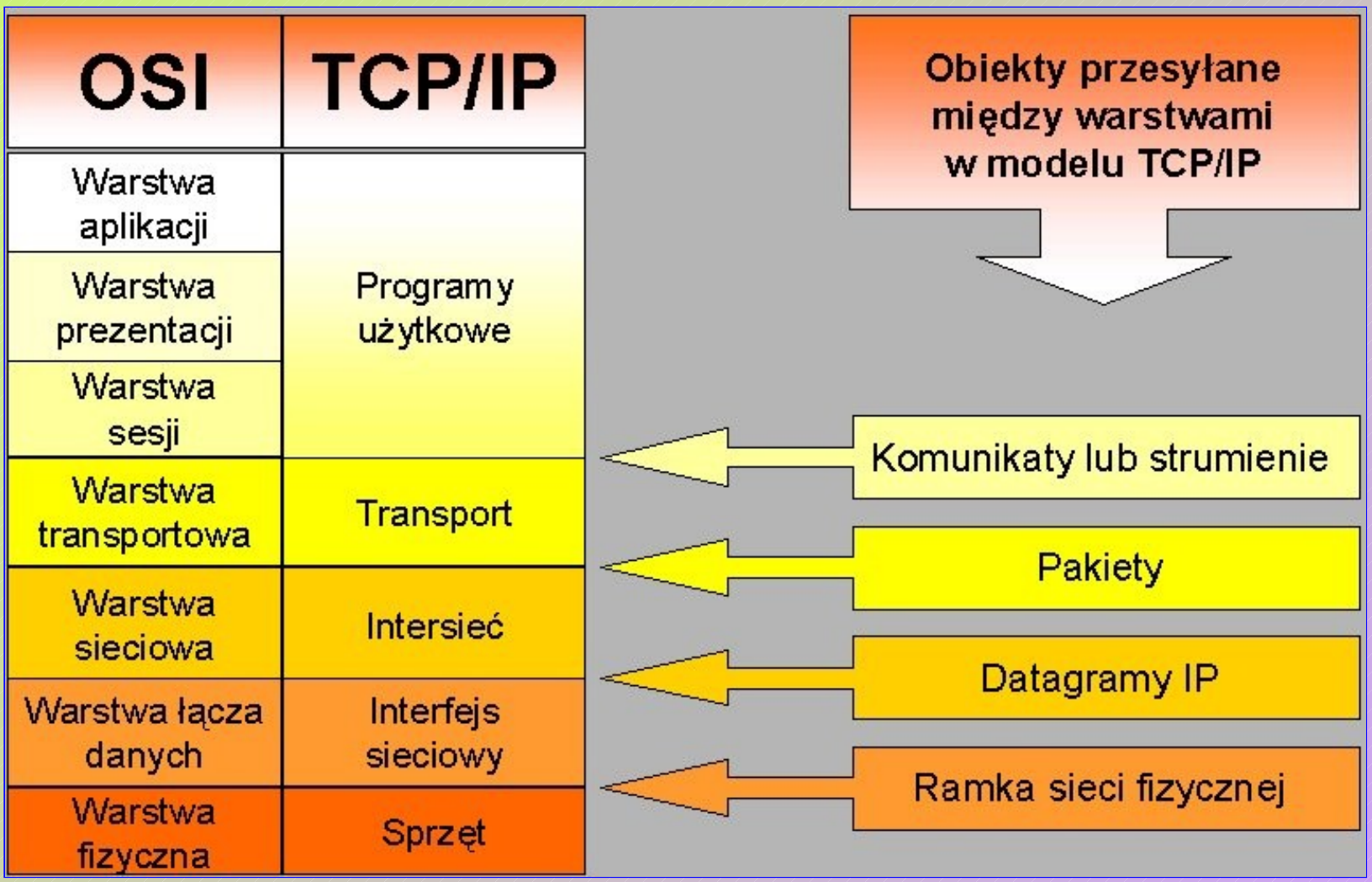
2. Warstwa międzysieciowa modelu TCP/IP odpowiada warstwie sieciowej modelu OSI (obie warstwy obsługują adresowanie i trasowanie).

Porównanie modeli OSI i TCP/IP

3. Warstwa transportu w każdym z modeli odpowiada za realizację sesji komunikacyjnych obejmujących całą drogę transmisji danych.

4. Warstwa aplikacji modelu TCP/IP łączy warstwy sesji, prezentacji danych i aplikacji modelu OSI. Model TCP/IP łączy w definicji aplikacji wszystkie zagadnienia związane z formatowaniem danych i zarządzaniem sesją.

Porównanie modeli OSI i TCP/IP



Protokoły model warstw TCP/IP

PROTOKOŁY WARSTWY MIĘDZYSIECIOWEJ

- Protokoły tej warstwy komunikują się z fizycznymi elementami sieci w warstwie interfejsu sieciowego albo zapewniają niezbędne informacje dla warstwy transportu. Są to:
  - Protokół Odwzorowania Adresów (**ARP** – *Address Resolution Protocol*);
  - Protokół Odwrotnego Odwzorowania Adresów (**RARP** – *Reverse Address Resolution Protocol*);

Protokoły model warstw TCP/IP

PROTOKOŁY WARSTWY MIĘDZYSIECIOWEJ

- Międzysieciowy Protokół Sterowania Komunikatami (**ICMP** – *Internet Control Message Protocol*);
- Protokół Międzysieciowy (**IP** – *Internet Protocol*);
- Międzysieciowy Protokół Komunikacji Grupowej (**IGMP** – *Internet Group Messaging Protocol*).

Protokoły model warstw TCP/IP

Protokół Odwzorowania Adresów ARP

- Odwzorowuje adres **IP** stacji docelowej na jej adres **MAC**.
- Zapewnia też stacji docelowej ustalenie adresu **MAC** nadawcy na podstawie jego adresu **IP**.
- Aby uniknąć procedury wielokrotnego odwzorowywania wykorzystywana jest pamięć podręczna ARP.
- Algorytm odwzorowywania zależny jest od tego czy obie stacje należą do tego samego segmentu sieci (stacje lokalne), czy też komunikacja dotyczy stacji odległej.

Protokoły model warstw TCP/IP

Protokół Odwzorowania Adresów ARP

- Algorytm odwzorowania dla stacji lokalnych:

1. Stacja wywołująca sprawdza zawartość pamięci podręcznej ARP poszukując adresu IP stacji docelowej;
2. W przypadku nie znalezienia odpowiedniego wpisu, stacja wywołująca tworzy pakiet ARP będący zapytaniem stacji docelowej o jej adres MAC.

Protokoły model warstw TCP/IP

Protokół Odwzorowania Adresów ARP

- Algorytm odwzorowania dla stacji lokalnych:

3. Pakiet zawiera adresy IP i MAC stacji źródłowej, dzięki czemu po jego odebraniu stacja docelowa może dodać je do swojej pamięci podręcznej.
4. Po odebraniu pakietu ARP porównuje zawarty w nim docelowy adres IP ze swoim własnym.

Protokoły model warstw TCP/IP

Protokół Odwzorowania Adresów ARP

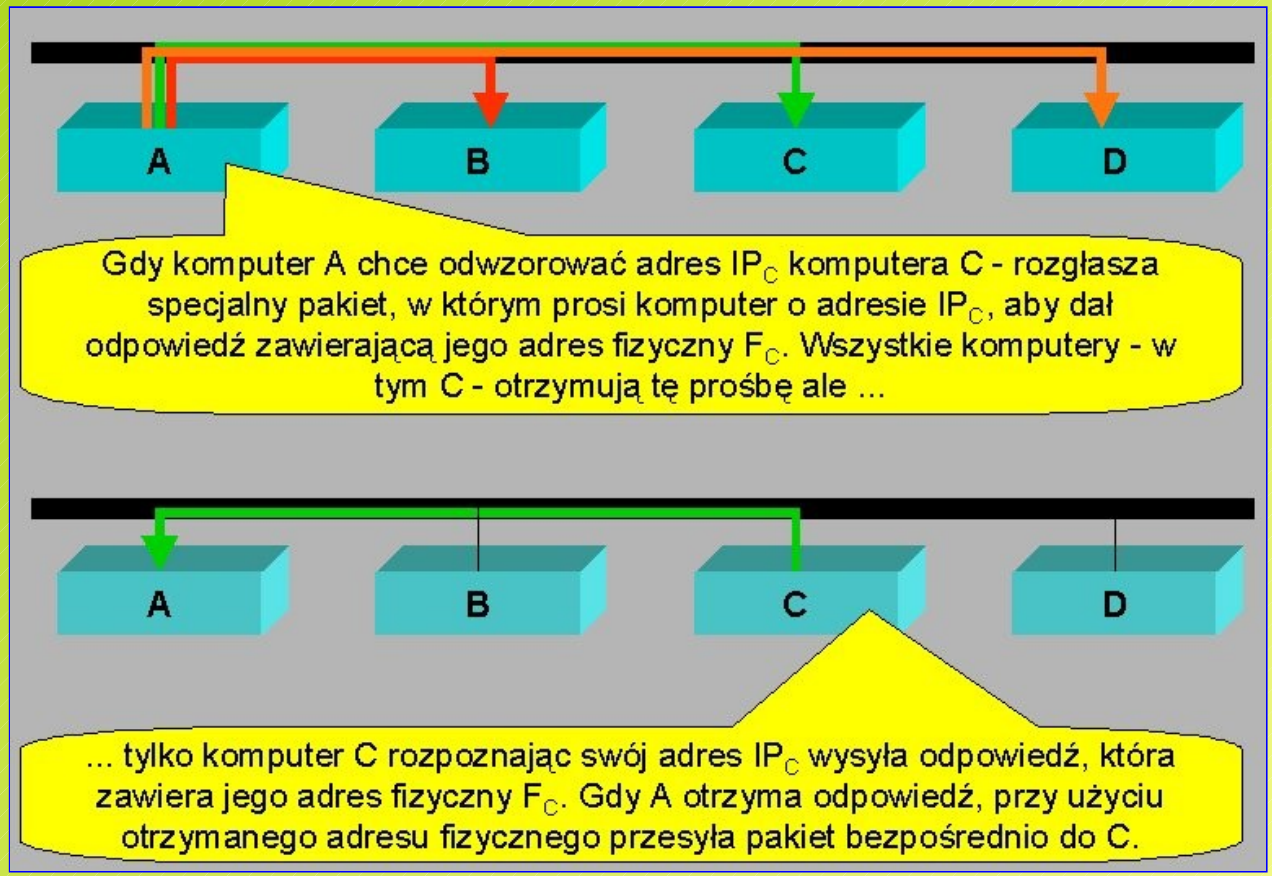
- Algorytm odwzorowania dla stacji lokalnych:

5. Gdy są zgodne wzbogaca zawartość swojej pamięci podręcznej ARP o oba adresy stacji źródłowej.
6. Stacja docelowa przygotowuje odpowiedź ARP zawierającą jej własne adresy MAC i IP, po czym wysyła je do stacji wywołującej.
7. Stacja źródłowa dopisuje otrzymane adresy MAC i IP do pamięci ARP.

Protokoły model warstw TCP/IP

Protokół Odwzorowania Adresów ARP

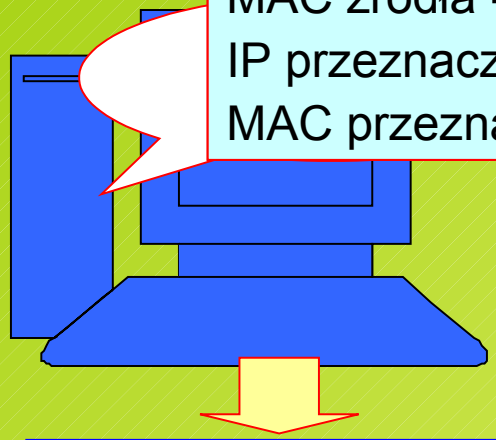
- Algorytm odwzorowania dla stacji lokalnych:



Protokoły model warstw TCP/IP

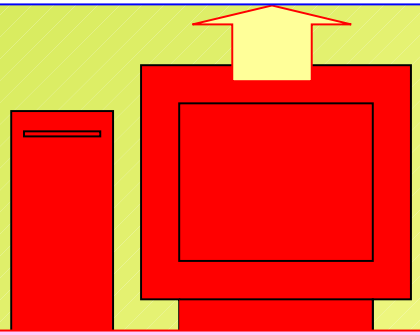
Protokół Odwzorowania Adresów ARP

- Adresacji lokalnych:



Zapytanie ARP
IP źródła = 172.16.1.4
MAC źródła = 00-80-37-CB-AA-45
IP przeznaczenia = 172.16.1.5
MAC przeznaczania = 00-00-00-00-0

Pamięć podręczna ARP
172.16.1.4 00-80-37-CB-AA-45



Pamięć podręczna ARP
172.16.1.3 00-80-35-BF-4E-AB
172.16.1.7 00-80-36-3B-A4-5D
172.16.1.5 00-80-DD-EE-12-3F

Odpowiedź ARP
IP źródła = 172.16.1.5
MAC źródła = 00-80-DD-EE-12-3f
IP przeznaczenia = 172.16.1.4
MAC przeznaczania = 00-80-37-CB-AA-45

Protokoły model warstw TCP/IP

Protokół Odwzorowania Adresów ARP

- Algorytm odwzorowania dla stacji odległych:

1. Stacja źródłowa wyszukuje w swoich ustawieniach TCP/IP adres bramy domyślnej.
2. Stacja przeszukuje pamięć podręczną ARP, sprawdzając, czy w ostatnim czasie określony został adres MAC bramy domyślnej. Jeżeli nie, wysyła pakiet ARP celem określenia jej adresu.

Protokoły model warstw TCP/IP

Protokół Odwzorowania Adresów ARP

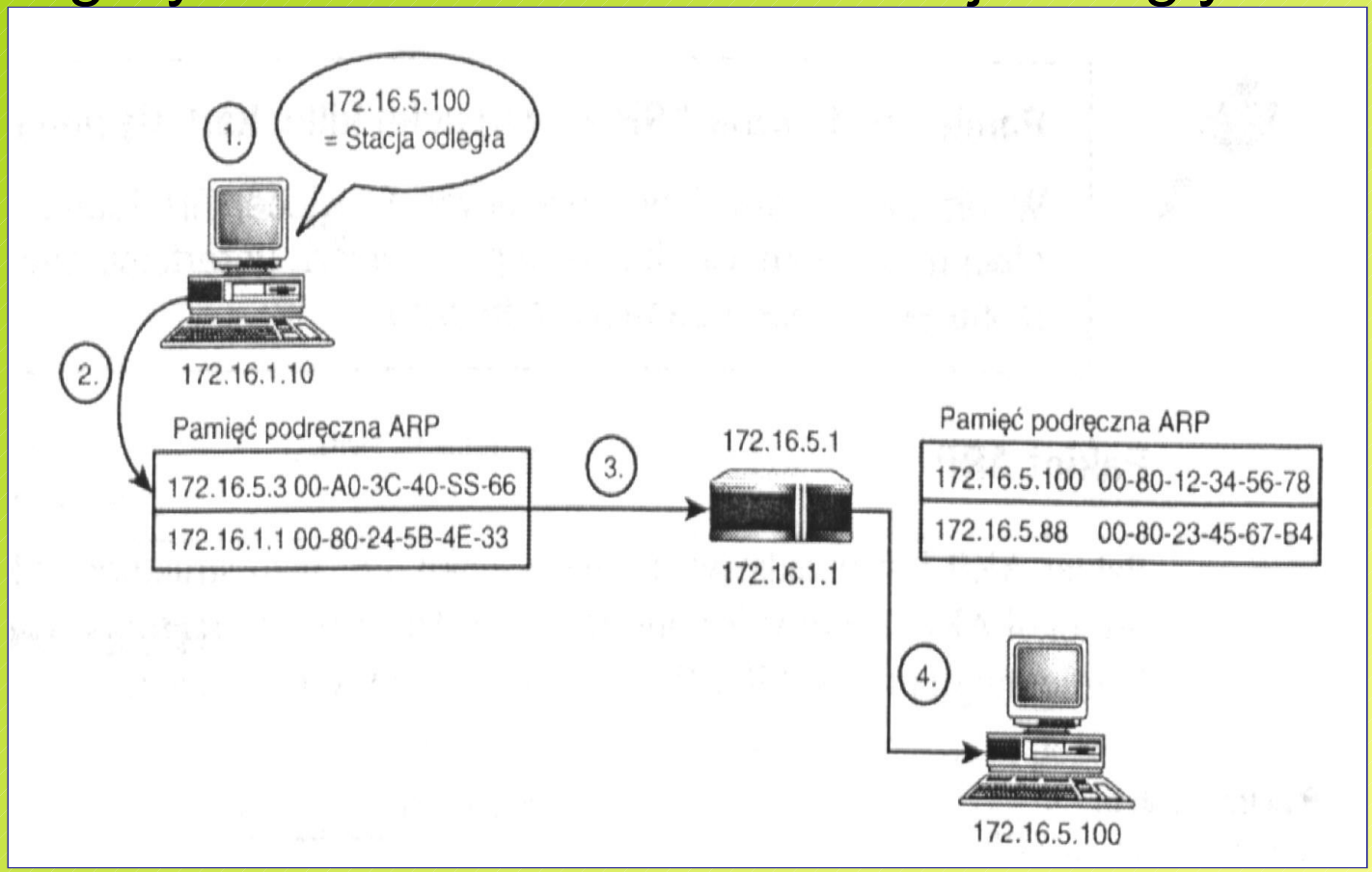
- Algorytm odwzorowania dla stacji odległych:

3. Dane są przesyłane do bramy domyślnej.
4. Brama domyślna sprawdza adres IP stacji docelowej wykonując algorytm działań podobny do wykonywanego przy połączeniu lokalnym.

Protokoły model warstw TCP/IP

Protokół Odwzorowania Adresów ARP

- Algorytm odwzorowania dla stacji odległych:



Protokoły model warstw TCP/IP

Protokół Odwzorowania Adresów ARP

UWAGA:

Jeżeli stacja wyposażona jest w kilka kart sieciowych to dla każdego przyłącza tworzona jest osobna pamięć podręczna ARP.

Protokoły model warstw TCP/IP

Pola pakietu ARP

Hardware Type (typ sprzętu)	Określa typ urządzeń wykorzystywanych w warstwie sieciowej
Protocol Type (typ protokołu)	Typ adresu umieszczanego w polach adresu protokołowego (dla adresów IP → 08-00)
Hardware Address Lenght (długość adresu sprzętowego)	Wyrażona w bajtach długość adresu sprzętowego. Dla sieci Ethernet i Token Ring jest to wartość 6.
Protocol Address Lenght (dł. adresu protokołowego)	Wyrażona w bajtach dł. adresu protokołowego. Dla protokołu Ipv4 jest to wartość 4.
Op Code (kod operacji)	Określa czy pakiet jest zapytaniem / odpowiedzią (1 - zapytanie ARP; 4- odpowiedź ARP)
Sender HW Address (adres sprzętowy nadawcy)	Adres sprzętowy stacji wysyłającej
Sender IP Address (adr. protokołowy nadawcy)	Adres IP stacji wysyłającej pakiet
Target HW Address (docelowy adres sprzętowy)	Adres sprzętowy stacji docelowej. W zapytaniu jest to 00-00-00-00-00-00
Target IP Address (docelowy adr. protokołowy)	Adres IP stacji docelowej

Protokoły model warstw TCP/IP

Polecenie ARP

- Wyświetla i modyfikuje wpisy w pamięci podręcznej ARP (*Address Resolution Protocol*), która zawiera jedną lub kilka tabel używanych do przechowywania adresów IP i odpowiednich rozpoznanych adresów fizycznych Ethernet lub Token Ring.
- Dla każdej karty sieciowej Ethernet lub Token Ring zainstalowanej na komputerze dostępna jest oddzielna tablica.
- Polecenie **arp** bez parametrów wyświetla „Pomoc”.

Protokoły model warstw TCP/IP

Polecenie ARP

- **Składnia**

arp [-a [*adres_intern*] [-N *adres_interf*]]
[-g [*adres_intern*] [-N *adres_interf*]]
[-d *adres_intern* [*adres_interf*]]
[-s *adres_intern adres_ethern*
[*adres_interf*]]

Protokoły model warstw TCP/IP

Polecenie ARP

- **Parametry**

-a [*adres_intern*] [-N *adres_interf*]

- Wyświetla bieżące tabele pamięci podręcznej ARP dla wszystkich interfejsów.
- Aby wyświetlić wpis pamięci podręcznej ARP dla określonego adresu IP, należy użyć polecenia arp -a z parametrem *adres_intern*, gdzie *adres_intern* jest adresem IP.

Protokoły model warstw TCP/IP

Polecenie ARP

- **Parametry**

-a [*adres_intern*] [-N *adres_interf*]

- Aby wyświetlić tabelę pamięci podręcznej ARP dla określonego interfejsu, należy użyć parametru -N *adres_interf*, gdzie *adres_interf* jest adresem IP przypisanym do interfejsu.
- W parametrze -N uwzględniana jest wielkość liter.

-g [*adres_intern*] [-N *adres_interf*]

- Działa identycznie jak -a.

Protokoły model warstw TCP/IP

Polecenie ARP

- **Parametry**

-d *adres_intern* [*adres_interf*]

- Usuwa wpis z określonym adresem IP, gdzie *adres_intern* jest adresem IP.
- Aby usunąć wpis w tabeli dla określonego interfejsu, należy użyć parametru *adres_interf*, gdzie *adres_interf* jest adresem IP przypisanym do interfejsu.
- Aby usunąć wszystkie wpisy, należy użyć symbolu wieloznacznego gwiazdki (*).

Protokoły model warstw TCP/IP

Polecenie ARP

- **Parametry**

-s ***adres_intern adres_ethern*** **[*adres_interf*]**

- Dodaje wpis statyczny do pamięci podręcznej ARP, który rozpoznaje adres fizyczny *adres_ethern* na podstawie adresu IP *adres_intern*.
- Aby dodać wpis statyczny pamięci podręcznej ARP do tabeli dla określonego interfejsu, należy użyć parametru *adres_interf*, gdzie *adres_interf* jest adresem IP przypisanym do interfejsu.

Protokoły model warstw TCP/IP

Polecenie ARP – przykłady:

- Wyświetla tabele pamięci podręcznej ARP dla wszystkich interfejsów:

  arp -a

- Wyświetla tabelę pamięci podręcznej ARP dla interfejsu, do którego przypisano adres IP 10.0.0.99:

  arp -a -N 10.0.0.99

- Dodaje wpis statyczny do pamięci podręcznej ARP, który rozpoznaje adres fizyczny 00-AA-00-4F-2A-9C na podstawie adresu IP 10.0.0.80:

  arp -s 10.0.0.80 00-AA-00-4F-2A-9C

Protokoły model warstw TCP/IP

WADY Protokół Odwzorowania Adresów ARP

- Jest zbyt kosztowny aby go używać za każdym razem gdy jakaś maszyna chce przesłać pakiet do innej: przy rozgłaszaniu każda maszyna w sieci musi taki pakiet przetworzyć.
- W celu zredukowania kosztów komunikacji komputery używające protokołu ARP przechowują w pamięci podręcznej ostatnio uzyskane powiązania adresu IP z adresem fizycznym, w związku z tym nie muszą ciągle korzystać z protokołu ARP.

Protokoły model warstw TCP/IP

WADY Protokół Odwzorowania Adresów ARP

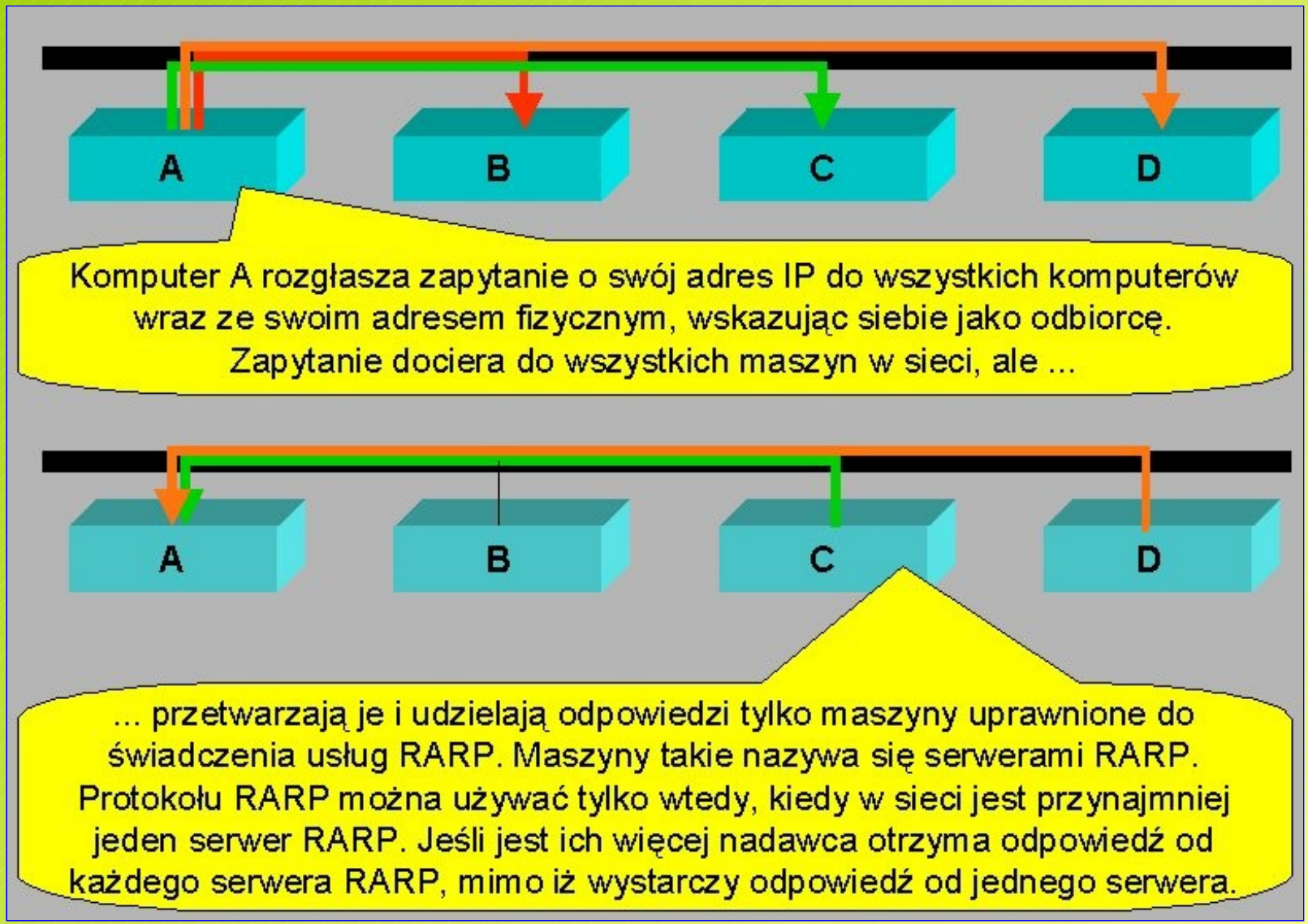
- Komputer A wysyłając prośbę o adres fizyczny komputera C dowiązuje informację o swoim adresie fizycznym. Ponieważ prośba ta dociera do wszystkich komputerów w sieci, mogą one umieścić w swoich pamięciach podręcznych informację o adresie fizycznym komputera A.
- Jeśli w komputerze zostanie zmieniony adres fizyczny (np. zmiana karty sieciowej), to może on bez zapytania o jego adres fizyczny rozgłosić go do innych komputerów, tak aby uaktualniły informacje w swoich pamięciach podręcznych.

Protokoły model warstw TCP/IP

Protokół Odwrotnego Odwzorowania Adresów RARP

- Protokół odwrotnego odwzorowania adresów **RARP** (*Reverse Address Resolution Protocol*) umożliwia uzyskiwanie adresu IP na podstawie znajomości własnego adresu fizycznego (pobranego z interfejsu sieciowego).
- Komputery bez dysku twardego pobierają adres IP z maszyny uprawnionej do świadczenia usług RARP, po przesłaniu zapytania z własnym adresem fizycznym.

Protokoły model warstw TCP/IP



Protokoły model warstw TCP/IP

ICMP – Internet Control Message Protocol

- Protokół **ICMP** zapewnia rodzinie protokołów TCP/IP mechanizm informowania o błędach oraz przesyłanie komunikatów sterujących.
- Gdy datagram powoduje błąd, ICMP może jedynie powiadomić pierwotnego nadawcę o przyczynie.
- Nadawca musi otrzymaną informację przekazać danemu programowi użytkownika, albo podjąć inne działanie mające na celu uporanie się z problemem.

Protokoły model warstw TCP/IP

ICMP – Internet Control Message Protocol

- Do funkcji pełnionych przez protokół ICMP należą:

1. Zapewnienie przesyłania sygnałów "*Echo Request / Echo Replay*", które sprawdzają niezawodność połączenia między stacjami (zwykle jest to realizowane poleceniem **PING** (*Packet Internet Gropher*).
2. Zmiana kierunku ruchu sieciowego, gdy jeden z routerów staje się przeciążony nadmierną ilością przesyłanych danych.

Protokoły model warstw TCP/IP

ICMP – Internet Control Message Protocol

- Do funkcji pełnionych przez protokół ICMP należą:

3. Rozsyłanie komunikatu o przekroczeniu czasu życia, gdy datagram osiągnął zerową wartość TTL i zostaje porzucony.
4. Rozsyłanie ogłoszeń dla routerów w celu ustalenia adresów wszystkich routerów w segmencie sieci.

Protokoły model warstw TCP/IP

ICMP – Internet Control Message Protocol

- Do funkcji pełnionych przez protokół ICMP należą:

5. Powiadomienie stacji o konieczności ograniczenia ilości przesyłanych danych, gdy ta przepełnia router lub sieciowe połączenie z siecią WAN.
6. Określenie, jaka maska podsieci jest używana w segmencie sieci.

Protokoły model warstw TCP/IP

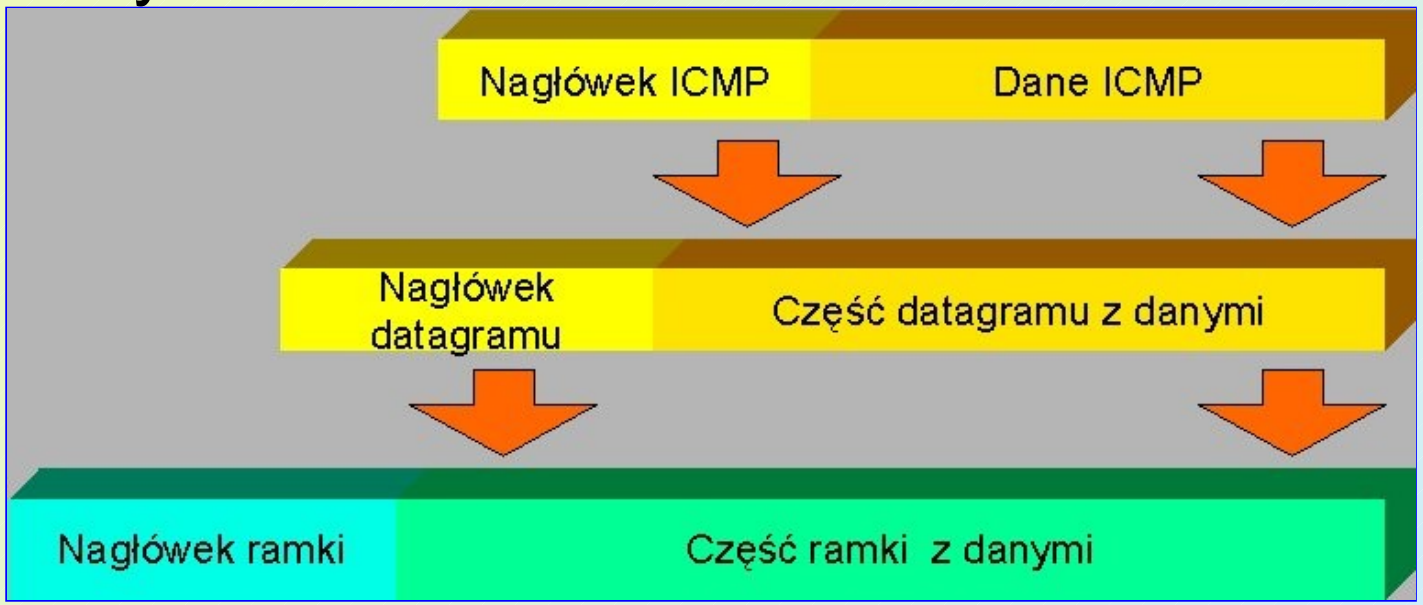
ICMP – Internet Control Message Protocol

- Każdy komunikat ICMP ma własny format, ale wszystkie zaczynają się trzema takimi samymi polami:
  - 8-bitowe pole TYP komunikatu identyfikuje komunikat,
  - 8-bitowe pole KOD daje dalsze informacje na temat rodzaju komunikatu,
  - Pole SUMA KONTROLNA (obliczane podobnie jak suma IP, ale suma kontrolna ICMP odnosi się tylko do komunikatu ICMP).

Protokoły model warstw TCP/IP

ICMP – Internet Control Message Protocol

- Oprócz tego komunikaty ICMP oznajmiające o błędach zawsze zawierają nagłówek i pierwsze 64 bity danych datagramu, z którym były problemy.



Protokoły model warstw TCP/IP

Pola pakietu ICMP

Type (typ)		8 bitowe pole wskazujące typ przesyłanego pakietu.
Code (kod)		Informacja dla stacji docelowej uzupełniająca pole Typ
Checksum (suma kontrolna)		Zapewnia wykrywanie błędów w części ICMP pakietu
Type-Specyfic Data (dane zależne od typu)	Długość zmienna	Zależnie od wykorzystania. Np. przy sprawdzaniu echa dane obejmują identyfikator i numer sekwencyjny.

Protokoły model warstw TCP/IP

Wykorzystanie ICMP w problemach z połączeniami

- Jednym z typowych problemów, z jakimi styka się administrator, jest wykrycie przyczyny powodującej, że stacja nie komunikuje się z siecią.
- W wielu przypadkach jest to niewłaściwa konfiguracja protokołu TCP/IP.
- Protokół ICMP może być pomocny w ustaleniu, który z parametrów konfiguracyjnych został błędnie ustawiony.

Protokoły model warstw TCP/IP

Wykorzystanie ICMP w problemach z połączeniami – przykład:

- **PING 127.0.0.1**
  ping na adres zarezerwowany - test poprawności zainstalowania rodziny protokołów TCP/IP
- **PING 172.16.2.200**
  wywołanie stacji testowej - test powiązania protokółu TCP/IP z właściwą kartą sieciową.

Protokoły model warstw TCP/IP

Wykorzystanie ICMP w problemach z połączeniami – przykład:

- **PING 172.16.2.1**
  wywołanie bramy domyślnej - test możliwości komunikowania się z innymi stacjami w tym samym segmencie.
- **PING 192.168.1.3**
  test połączenia ze stacją odległą.

Protokoły model warstw TCP/IP

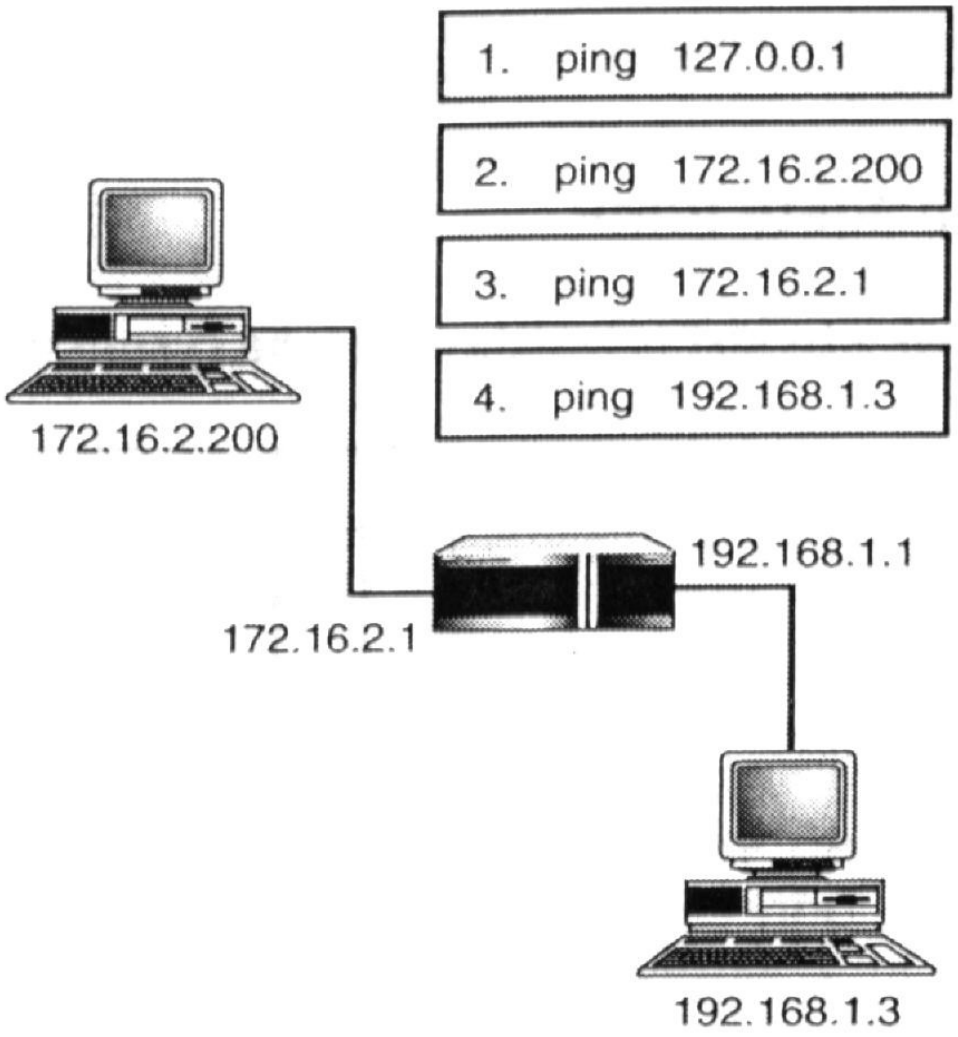
Wykorzystanie ICMP
w problemach
z połączeniami :

PING 127.0.0.1

PING 172.16.2.200

PING 172.16.2.1

PING 192.168.1.3



Protokoły model warstw TCP/IP

Polecenie PING

- **Składnia**

ping [**-t**] [**-a**] [**-n** *liczba*] [**-l** *długość*] [**-f**] [**-i** *ttl*]
[**-v** *tos*] [**-r** *liczba*] [**-s** *liczba*]
[[**-j** *lista_komputerów*] |
[**-k** *lista_komputerów*]]
[**-w** *czas_wygaśnięcia*] *lista_docelowa*

Protokoły model warstw TCP/IP

Polecenie PING

- **Parametry**

- **-t** wysyła pakiety kontrolne do określonego komputera aż do chwili przerwania połączenia.
- **-a** rozwiązuje adresy do nazw komputerów.
- **-f** przesyła w pakiecie flagę zakazującą fragmentacji (Do not Fragment). Pakiet nie będzie na trasie fragmentowany przez bramy.
- **-n** *liczba* wysyła liczbę pakietów ECHO zgodną z parametrem *liczba*. Wartość domyślna jest równa 4.

Protokoły model warstw TCP/IP

Polecenie PING

- **Parametry**

-l *długość*	wysyła pakiety ECHO zawierające ilość danych określoną przez parametr *długość*. Domyślna ilość to 32 bajty, (maksymalnie 65 527 bajty)
-i *ttl*	ustawia czas życia datagramu (*Time To Live*)
-v *tos*	ustawia w polu typu usługi (*Type Of Service*) wartość określoną przez parametr *tos*.

Protokoły model warstw TCP/IP

IP – Internet Protocol

-
-
-

Protokoły model warstw TCP/IP

IP – Internet Protocol

- IP

1.

2.

Protokoły model warstw TCP/IP

IP – Internet Protocol

- IP

3.

Protokoły model warstw TCP/IP

Datagram IP

- Datagram

- nagłówek dane
- adres nadawcy

  odbiorcy pole typu

-

Protokoły model warstw TCP/IP

Datagram IP

-

nie są uwarunkowane sprzętowo

Version (nr wersji IP)	**Length** (długość nagł.)	**Service Type** (typ obsługi)	**Packet Length** (długość całego pakietu IP)	
Identification (identyfikator określający datagram początkowy)			**Flags** (znacznik frag.)	**Fragment Offset** (pozycja fragmentu)
Time-to-Live (czas istnienia datagramu w sieci)		**Protocol** (nazwa prot.)	**Header Checksum** (suma kontrolna nagłówka)	
Source Address (32 bitowy adres IP stacji źródłowej)				
Destination Address (32 bitowy adres IP stacji docelowej)				
Options (opcje)				**Padding** (dopełnienie)
DANE				

Protokoły model warstw TCP/IP

Datagram IP – opis pól:

- Pole WERSJA

Protokoły model warstw TCP/IP

Datagram IP – opis pól:

- **Pole DŁUGOŚĆ NAGŁÓWKA**
- **Pole OPCJE IP UZUPEŁNIENIE**
- **Pole DŁUGOŚĆ CAŁKOWITA**

Protokoły model warstw TCP/IP

Datagram IP – opis pól:

- **Pole TYP OBSŁUGI**

- **Podpole PIERWSZEŃSTWO**

Protokoły model warstw TCP/IP

Datagram IP – opis pól:

- Pole TYP OBSŁUGI

- Bity O, S, P
  - O
  - S
  - P

Protokoły model warstw TCP/IP

Datagram IP – opis pól:

- **Pole CZAS ŻYCIA TTL** *Time To Live*
  -

Protokoły model warstw TCP/IP

Datagram IP – opis pól:

-
-
-

Protokoły model warstw TCP/IP

Datagram IP – opis pól:

- **Pole PROTOKÓŁ**

Internet Network Information Center INTERNIC

-
-
-

Protokoły model warstw TCP/IP

Datagram IP – opis pól:

- Pole SUMA KONTROLNA NAGŁÓWKA
-
-
-

Protokoły model warstw TCP/IP

Datagram IP – opis pól:

- Pola ADRES IP NADAWCY ADRES IP ODBIORCY

- Pole OPCJE IP

-

Protokoły model warstw TCP/IP

Datagram IP – opis pól:

- KLASA OPCJI

Klasa opcji	Znaczenie
0	Kontrola datagramów lub sieci
1	Zarezerwowane do przyszłego użytku
2	Poprawianie błędów i pomiary
3	Zarezerwowane do przyszłego użytku

Protokoły model warstw TCP/IP

Datagram IP – opis pól:

Klasa opcji	Numer opcji	Długość	Opis
0	0	-	Koniec listy opcji. Używana gdy opcje nie kończą się wraz z końcem nagłówka.
0	1	-	Bez przypisanej funkcji - wypełnienie
0	2	11	Tajność - używana do zastosowań wojskowych
0	3	zmienna	Swobodne trasowanie wg nadawcy - używana do prowadzenia datagramu określoną ścieżką.
0	7	zmienna	Zapisuj trasę - używana do śledzenia trasy.
0	9	zmienna	Rygorystyczne trasowanie wg nadawcy - używana do ścisłego prowadzenia datagramu.
2	4	zmienna	Intersieciowy datownik - używana do zapisywania czasów wzdłuż ścieżki.

Protokoły model warstw TCP/IP

Datagram IP – koleje życia datagramu:

-
  -
  -
  -
    nagłówku IP
  -
  -

Protokoły model warstw TCP/IP

Datagram IP – koleje życia datagramu:

-
  -
  -
  -

Protokoły model warstw TCP/IP

Datagram IP – koleje życia datagramu:

-
-
-

Protokoły model warstw TCP/IP

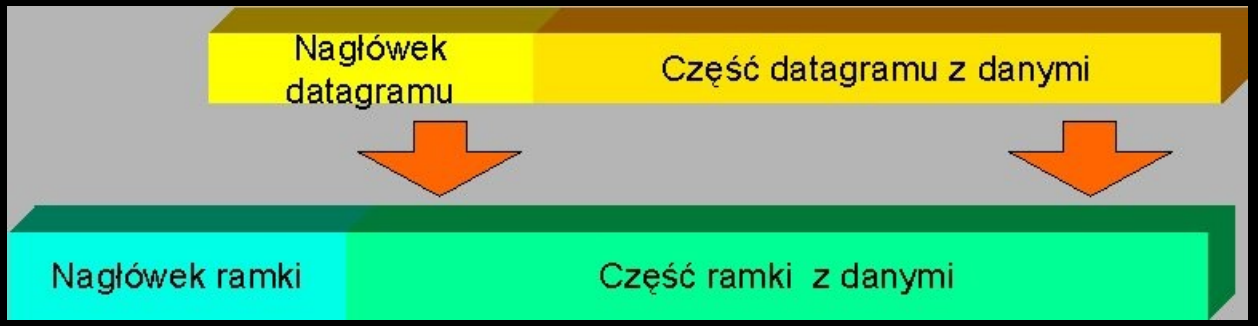
Datagram IP – koleje życia datagramu:

-
  -
  -
  -
  -

Protokoły model warstw TCP/IP

Datagram IP – kapsułkowanie

- *encapsulation*



Protokoły model warstw TCP/IP

Datagram IP – fragmentacja

-
-
-

maksymalnej jednostki transmisyjnej danej sieci *maximum Transfer Unit - MTU*

Protokoły model warstw TCP/IP

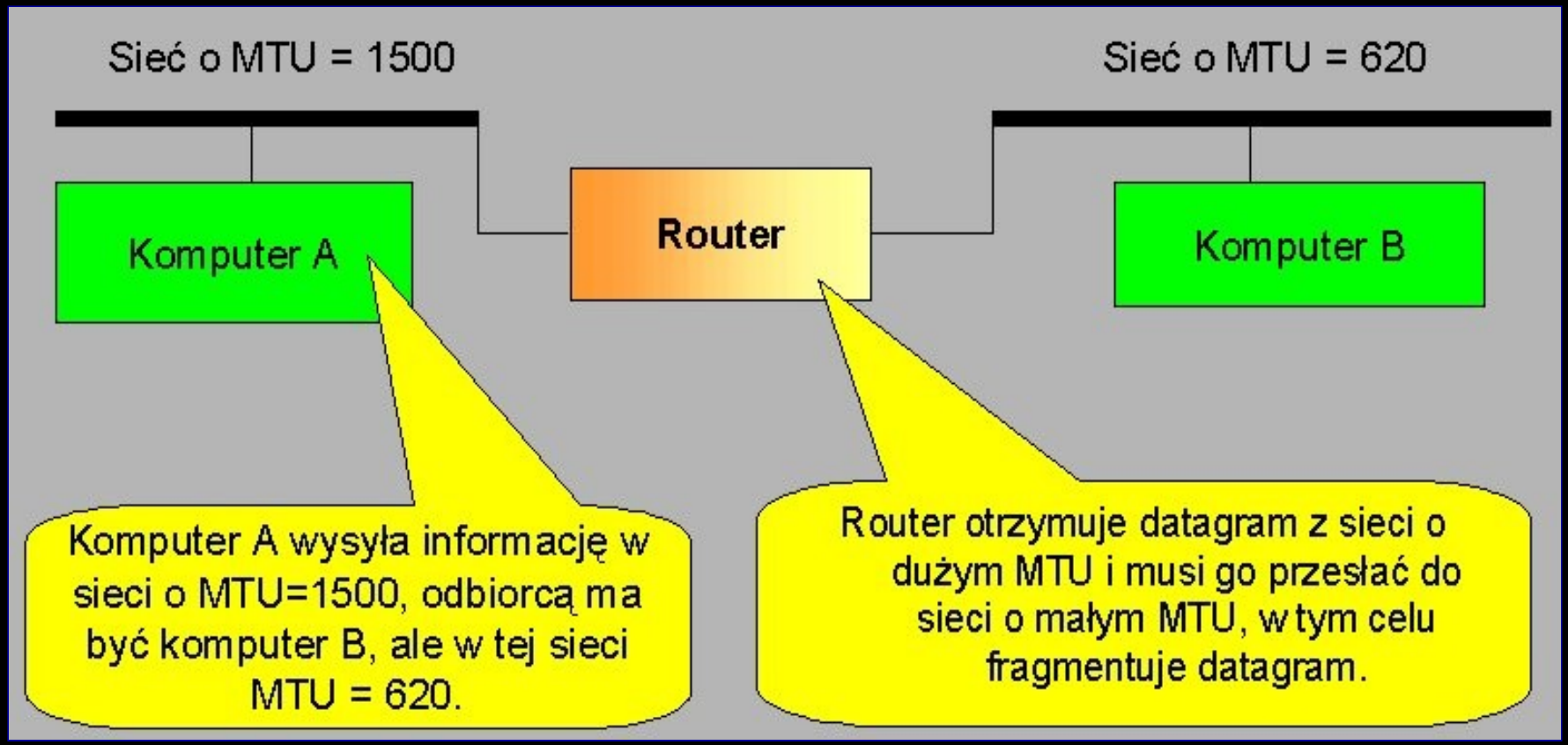
Datagram IP – fragmentacja

-
-
-

z wyjątkiem pola
ZNACZNIKI, które wskazuje, że jest to fragment

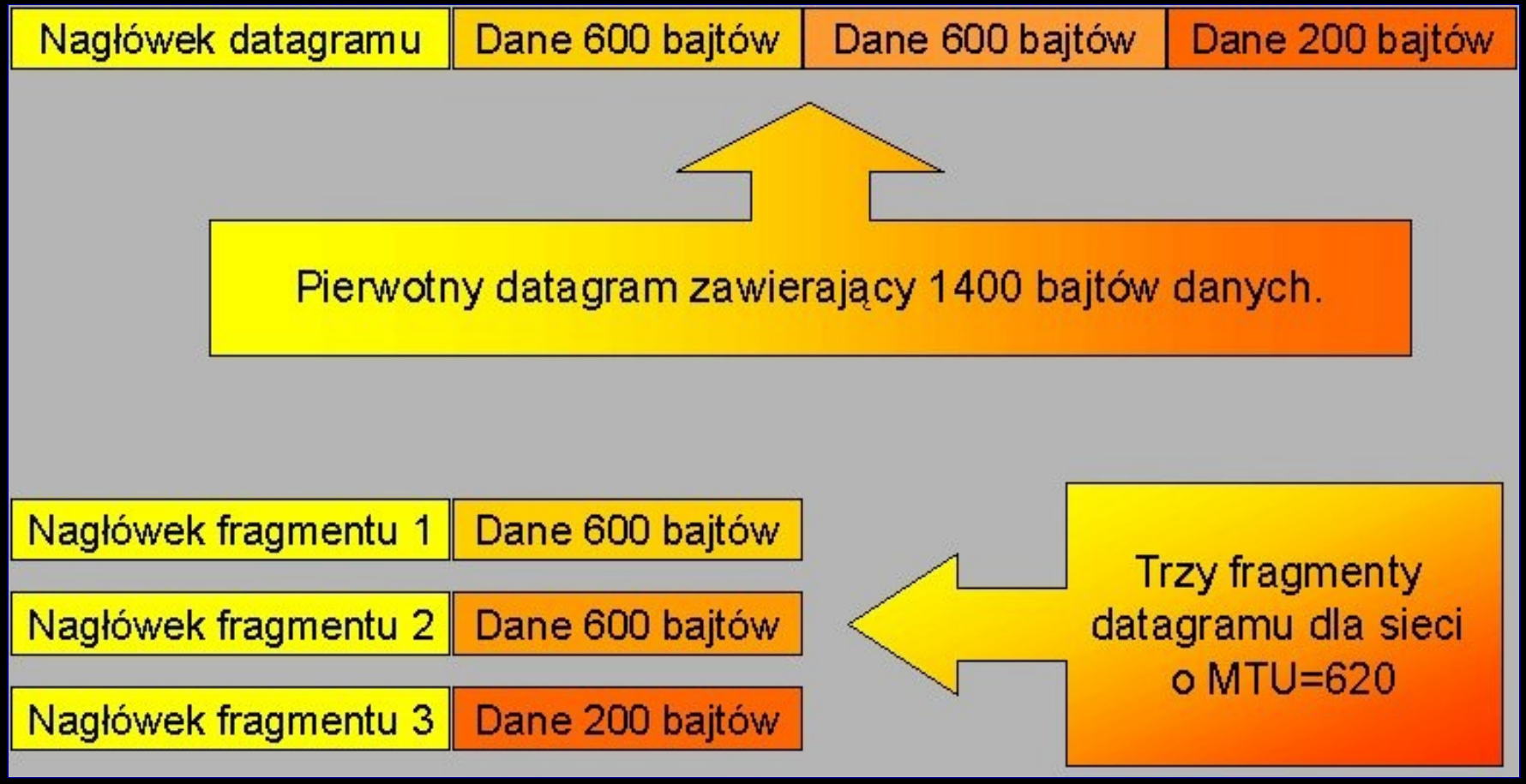
Protokoły model warstw TCP/IP

Datagram IP – fragmentacja

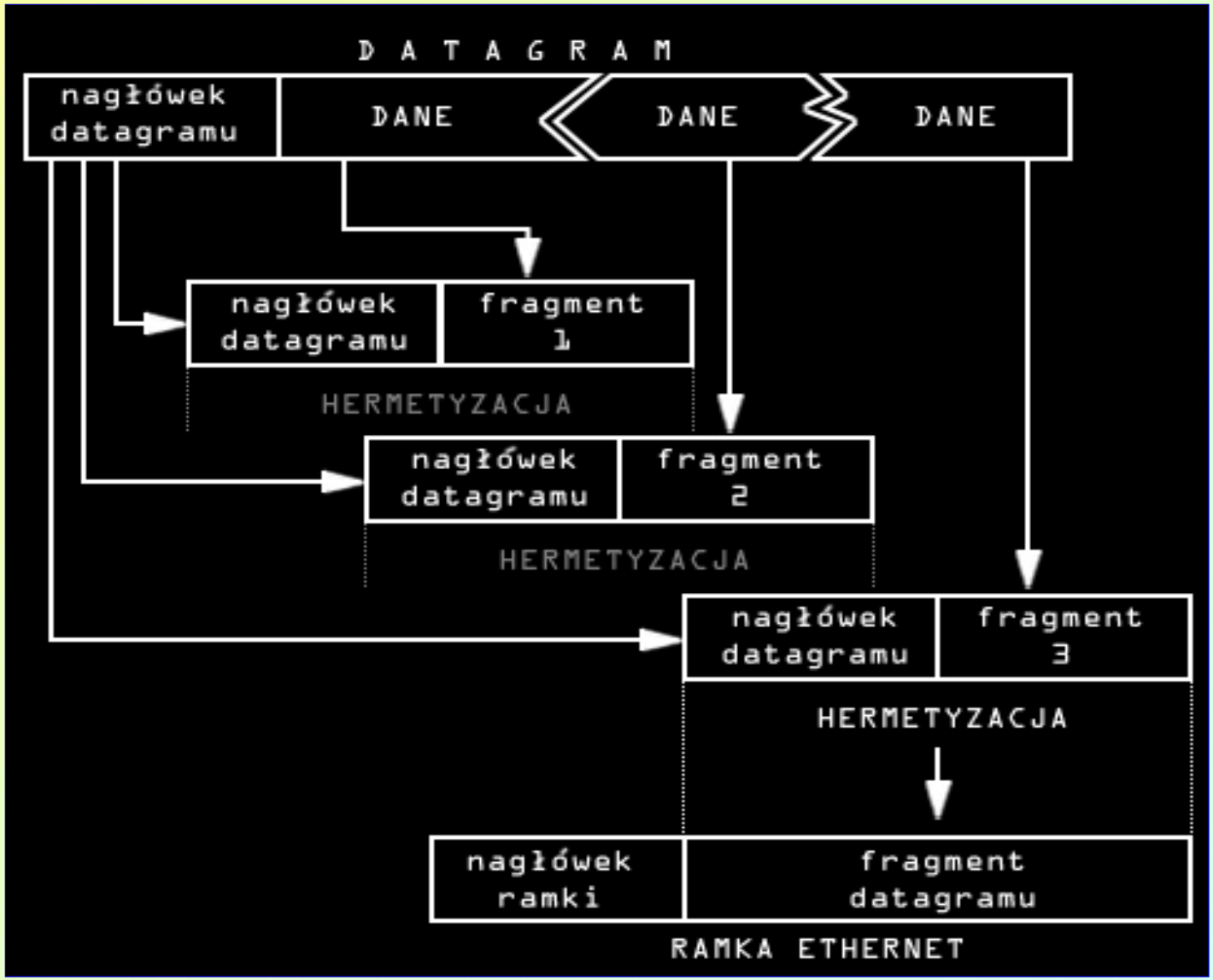


Protokoły model warstw TCP/IP

Datagram IP – fragmentacja



Protokoły model warstw TCP/IP



Protokoły model warstw TCP/IP

Datagram IP – kontrola fragmentacji

-

IDENTYFIKACJA ZNACZNIKI PRZESUNIĘCIE FRAGMENTU

- Pole IDENTYFIKACJA

wszystkie kawałki będące częściami tego samego datagramu posiadają ten sam identyfikator

Protokoły model warstw TCP/IP

Datagram IP – kontrola fragmentacji

- Pole ZNACZNIKI
  -
  -
  -

Protokoły model warstw TCP/IP

Datagram IP – kontrola fragmentacji

- Pole PRZESUNIĘCIE FRAGMENTU

Protokoły model warstw TCP/IP

IGMP – Internet Group Messaging Protocol

- **Międzysieciowy Protokół Komunikacji Grupowej** pozwala na wysyłanie informacji do wielu stacji docelowych jednocześnie.
- Informację taką można wysłać do określonej grupy komputerów.
- Pakiety są dostarczane za pomocą protokółu UDP.

Protokoły model warstw TCP/IP

IGMP – Internet Group Messaging Protocol

- Mechanizm multiemisji posiada kilka istotnych cech:
  - Adresowanie multiemisji jest oparte na adresach IP **klasy D** (od **244.0.0.1** do **239.255.255.255**);
  - Adres **244.0.0.1** jest zarezerwowany dla grupy „wszystkie stacje” (wszystkie stacje i routery segmentu sieciowego);

Protokoły model warstw TCP/IP

Pola pakietu IGMP

Version (nr wersji)	**Type** (zapyt./odpow.)	(nie wykorzyst.)	**Checksum** (suma kontrolna)
Group Address (32 bitowy adres IP grupy, w której stacja zgłasza członkostwo; w przypadku zapytania pole puste)			

Adresowanie IP

- Adresy IP są niepowtarzalnymi identyfikatorami wszystkich stacji należących do intersieci TCP/IP.
- Adres IP jest 32-bitową liczbą całkowitą zawierającą informacje o tym do jakiej sieci włączony jest dany komputer, oraz jednoznaczny adres w tej sieci.
- Adres zapisywany jest on w postaci czterech liczb dziesiętnych oddzielonych kropkami.
- Każda liczba odpowiada 8 bitom adresu IP.

Adresowanie IP

10000000	00001010	00000010	00011110
128	10	2	30

- Adresy IP podzielone są na klasy.
- Klasa adresu IP określona jest przez najstarsze bity, przy czym do zidentyfikowania jednej z trzech zasadniczych klas (A, B, C) wystarczą dwa pierwsze bity.
- Taki mechanizm adresowania wykorzystują routery, które używają adresu sieci do wyznaczania trasy pakietów.

Adresowanie IP

Przydzielanie adresów IP

- W celu zapewnienia jednoznaczności identyfikatorów sieci, wszystkie adresy przydzielane są przez jedną organizację.
- Zajmuje się tym Internet Network Information Center (**INTERNIC**).
- Przydziela ona adresy sieci, zaś adresy maszyn administrator może przydzielać bez potrzeby kontaktowania się z organizacją.

Adresowanie IP

Przydzielanie adresów IP

- Organizacja ta przydziela adresy tym instytucjom, które są lub będą przyłączone do ogólnoświatowej sieci INTERNET.
- Każda instytucja może sama wziąć odpowiedzialność za ustalenie adresu IP, jeśli nie jest połączona ze światem zewnętrznym.
- Nie jest to jednak dobre rozwiązanie, gdyż w przyszłości może uniemożliwić współpracę między sieciami i sprawiać trudności przy wymianie oprogramowania z innymi ośrodkami.

Adresowanie IP

Klasy adresów IP

- Wewnątrz pojedynczego segmentu sieci wszystkie stacje korzystają ze wspólnego adresu sieci, a jedynie jego część identyfikuje pojedynczą stację.
- Obserwując najstarsze bity adresu można stwierdzić do jakiej klasy należy dany adres, w efekcie można stwierdzić ile bitów będzie adresowało sieć, ile zaś sam komputer.
- W zależności od liczby pól identyfikujących stację wyróżnia się pięć klas adresów.

Adresowanie IP

Klasy adresów IP

Adresowanie IP

Klasy adresów IP – klasa A

- 8 bitów adresu wskazuje numer sieci, pozostałe 24 określają pracująca w niej stację.
- Można za jej pomocą opisać 126 sieci o mocy 16 777 214 stacji.
- Ograniczenia:
  - identyfikatorem sieci nie może być liczna 0 i zarezerwowana dla pętli zwrotnej liczba 127;
  - identyfikator stacji nie może składać się z samych zer i samych jedynek.

Adresowanie IP

Klasy adresów IP – klasa B

- W klasie B 16 bitów określa sieć, a kolejne 16 stację.
- Wartość w pierwszym oktecie mieści się między 128 a 191.
- Biorąc pod uwagę, że pierwsze dwie cyfry pierwszego oktetu to 1 i 0 na pozostałych 14 bitach można opisać 16 384 sieci po $(2^{16} – 2)$=65 534 stacje każda.

Adresowanie IP

Klasy adresów IP – klasa C

- Z siecią związane są 24 bity, a ze stacjami 8 bitów.
- Wartość pierwszego oktetu mieści się w granicach od 192 do 223.
- Ze względu na wyłączenie pierwszych trzech cyfr adresu (110) pozwala to na zdefiniowanie 97 152 sieci po 254 stacje każda.

Adresowanie IP

Klasy adresów IP – klasa D

- To grupa adresów przeznaczonych do wykorzystania przez grupy multisesji i nie może być wykorzystana do oznaczenia pojedynczej stacji.

Klasy adresów IP – klasa E

- Adresy zarezerwowane do użytku w przyszłości, wykorzystywane są jedynie do celów eksperymentalnych i nie są dostępne publicznie.

Adresowanie IP

Ogólne zasady adresowania IP

1. Wszystkie stacje w jednym fizycznym segmencie sieci powinny mieć ten sam identyfikator sieci.
2. Część adresu IP określająca pojedynczą stację musi być odmienna dla każdej stacji w segmencie sieci.
3. Identyfikatorem sieci nie może być **127** – wartość zarezerwowana dla celów diagnostycznych.

Adresowanie IP

Ogólne zasady adresowania IP

4. Identyfikator sieci nie może składać się z samych jedynek (binarnie)- jest to adres rozgłaszania.
5. Identyfikator stacji nie może również składać się z samych jedynek (binarnie)- jest to adres rozgłaszania dla sieci.
6. Identyfikator sieci nie może składać się z samych zer (binarnie)- jest to oznaczenie sieci lokalnej.

Adresowanie IP

Ogólne zasady adresowania IP

7. Identyfikator stacji również nie może składać się z samych zer (binarnie)- jest to oznaczenie sieci wskazywanej przez pozostałą część adresu i nie może zostać przypisany pojedynczej stacji.

Adresowanie IP

Adresy specjalne IP

- Identyfikatory z binarnymi jedynkami w miejscu adresu stacji są adresami rozgłaszania.
- Adres IP: 255.255.255.255 jest zarezerwowany jako adres ograniczonego rozgłaszania i może być użyty, gdy stacja nie zna identyfikatora sieci

  (*ogólną zasadą konfigurowania routerów jest uniemożliwienie przesyłania takiego zgłoszenia poza lokalny segment sieci*).

Adresowanie IP

Adresy specjalne IP

- Adres sieci 127 jest zarezerwowany dla celów diagnostycznych (tzw. *loopback address* – adres pętli zwrotnej).
- Adres IP: 0.0.0.0 oznacza po prostu tyle, co „niniejsza stacja”.

Adresowanie IP

Maski podsieci

- Maska podsieci (**SNM** – *subnet mask*) jest wykorzystywana do określenia, ile bitów adresu IP wskazuje sieć a ile stację w tej sieci.
- Dla klas A, B, C są wykorzystywane maski domyślne:

Klasa A	**255.0.0.0**	adres sieci pierwsze 8 bitów
Klasa B	**255.255.0.0**	adres sieci pierwsze 16 bitów
Klasa C	**255.255.255.0**	adres sieci pierwsze 24 bity

Adresowanie IP

Maski podsieci - przeznaczenie

- Stacja źródłowa używa maski podsieci do określenia, czy stacja docelowa znajduje się w sieci lokalnej czy odległej.
- Obliczany jest wówczas iloczyn logiczny (AND) adresu każdej ze stacji i adresu maski podsieci.
- Jeżeli wyniki obu operacji są identyczne oznacza to, że stacja docelowa należy do tej samej sieci lokalnej.
- Jeżeli wyniki są różne dane kierowane są do routera wskazanego w tabeli tras stacji źródłowej.

Adresowanie IP

Maski podsieci - przeznaczenie

Adres IP stacji źródłowej	10101100 00010000 00000010 00000100
Maska podsieci stacji źródłowej	11111111 11111111 00000000 00000000
Wynik koniunkcji	10101100 00010000 00000000 00000000

Adres IP stacji docelowej	10101100 00010000 00000011 00000101
Maska podsieci stacji źródłowej	11111111 11111111 00000000 00000000
Wynik koniunkcji	10101100 00010000 00000000 00000000

Adresowanie IP

Maski podsieci – maski niestandardowe

- Jeżeli zachodzi konieczność wydzielenia w obrębie sieci, kilku podsieci można wykorzystać w tym celu maski niestandardowe.
- Maski takie tworzy się wykorzystując w celu identyfikacji podsieci początkową część bitów identyfikujących stacje.

Przykład:

M. sieci	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
255.255.0.0	sieć								sieć								stacja								stacja							

M. podsieci	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
255.255.240.0	sieć								sieć								sieć				stacja				stacja							

Adresowanie IP

Maski podsieci – problemy z maskowaniem

- Objawy niepoprawnego maskowania mogą być następujące:
  - Brak dostępu do stacji odległych przy jednoczesnym zachowaniem dostępu do sieci lokalnej.
  - W sieci odległej dostępne są wszystkie stacje z wyjątkiem jednej.
  - Brak możliwości komunikacji ze stacją w sieci lokalnej - jest rozpoznawana jako stacja w sieci odległej.

Protokoły model warstw TCP/IP

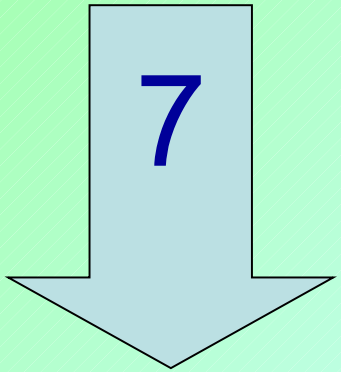
PROTOKOŁY WARSTWY TRANSPORTOWEJ

- Na bazie protokołu internetowego (IP) zbudowane są dwa protokoły warstwy transportowej:
  - **UDP** (User Datagram Protocol) - protokół bezpołączeniowy, zawodny;
  - **TCP** (Transmission Control Protocol) - protokół połączeniowy, niezawodny.

Protokoły model warstw TCP/IP

PROTOKOŁY WARSTWY TRANSPORTOWEJ

- Usługi oferowane w tej warstwie w większości są opcjonalne - żadna z nich nie jest obowiązkowa, ponieważ nie wszystkie aplikacje potrzebują wszystkich usług.
- Pełna lista oferowanych usług obejmuje:



Protokoły model warstw TCP/IP

PROTOKOŁY WARSTWY TRANSPORTOWEJ

1. Podstawowy transfer danych (*basic data transfer*) - przesyła ciągi oktetów w obu kierunkach transmisji.
   - Oktety przed transmisją pakowane są w segmenty danych.
   - Protokół sam decyduje czy blok danych należy wysłać czy poczekać na jeszcze większą porcję.

Protokoły model warstw TCP/IP

PROTOKOŁY WARSTWY TRANSPORTOWEJ

2. Wiarygodność transmisji (*reliability*) - ma za zadanie naprawić wszystkie błędy jakie mogły pojawić się w niższej warstwie.
   - Musi zapewnić odzyskanie danych, które zostały zagubione, zniekształcone, zniszczone, zduplikowane, albo dostarczone w niewłaściwej kolejności.
   - System zapewnia, że błędy w transmisji nie powinny mieć wpływu na poprawność przesyłanych danych.

Protokoły model warstw TCP/IP

PROTOKOŁY WARSTWY TRANSPORTOWEJ

3. Kontrola przepływu (*flow control*) - komputer odbierający może sterować ilością danych wysyłanych przez komputer źródłowy wysyłając z każdym sygnałem potwierdzającym (*ACK*) tzw. okna, które informują komputer wysyłający ile jeszcze oktetów może wysłać przed otrzymaniem kolejnego pozwolenia.
   - Bez kontroli przepływu szybszy komputer mógłby zalać każdego hosta taką ilością informacji z jaką tamten mógłby sobie nie poradzić.

Protokoły model warstw TCP/IP

PROTOKOŁY WARSTWY TRANSPORTOWEJ

4. Multipleksowanie (*multiplexing*)
   - Ponieważ zwykle działa wiele programów, procesów, które potrzebują skorzystać z usług TCP/IP trzeba im umożliwić równoczesne korzystanie z sieci.
   - W tym celu TCP udostępnia dodatkowy zbiór adresów (inaczej portów) przypisywanych konkretnym procesom.
   - Numer portu w połączeniu z adresem sieci i hosta tworzy tzw. gniazdo (*socket*), a para gniazd identyfikuje każde połączenie.

Protokoły model warstw TCP/IP

PROTOKOŁY WARSTWY TRANSPORTOWEJ

5. Połączenia (*connections*) – wykorzystywane mechanizmy wymagają najpierw zainicjowania a potem utrzymywania pewnych informacji statusowych dotyczących każdego przesyłanego strumienia danych.
   - Kiedy dwa procesy mają zacząć komunikację muszą najpierw nawiązać połączenie (czyli wymienić informację statusową) a po zakończeniu komunikacji połączenie jest zamykane w celu zwolnienia zasobów

Protokoły model warstw TCP/IP

PROTOKOŁY WARSTWY TRANSPORTOWEJ

6. Dostarczenie w tej samej kolejności (*same order delivery*)
   - Warstwa sieciowa nie gwarantuje, że pakiety danych dotrą w tej samej kolejności w jakiej zostały wysłane, ale często jest to pożądana właściwość i zapewnia ją warstwa transportowa.
   - Najprostszym sposobem jest danie każdemu pakietowi numeru i pozwolenie odbiorcy na powtórne zamówienie pakietów.

Protokoły model warstw TCP/IP

PROTOKOŁY WARSTWY TRANSPORTOWEJ

7. Przetworzenie na strumień bajtów (*byte orientation*).
   - Zamiast operowania na zestawach pakietów warstwa transportowa może umożliwić komunikację przez strumień bajtów.

Protokół UDP

- W zestawie protokołów TCP/IP protokół datagramów użytkownika **UDP** (*User Datagram Protocol*), zapewnia porty protokołów używane do rozróżniania programów wykonywanych na pojedynczej maszynie.
- Oprócz wysyłanych danych, każdy komunikat zawiera numer portu odbiorcy i numer portu nadawcy, dzięki czemu oprogramowanie UDP odbiorcy może dostarczyć komunikat do właściwego adresata.

Protokół UDP

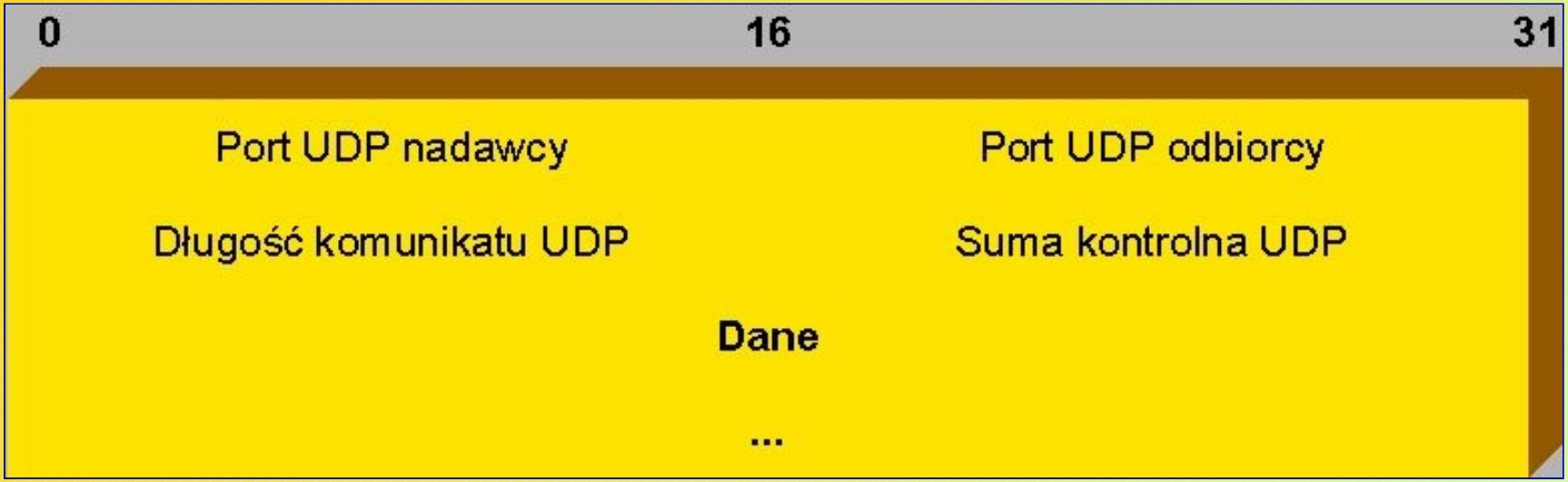
- Do przesyłania komunikatów między maszynami UDP używa podstawowego protokołu IP i ma tę samą niepewną, bezpołączeniową semantykę dostarczania datagramów co IP - nie używa potwierdzeń w celu upewnienia się, o dotarciu komunikatów i nie zapewnia kontroli szybkości przesyłania danych między maszynami.
- Z tego powodu komunikaty UDP mogą być gubione, duplikowane lub przychodzić w innej kolejności niż były wysłane, ponadto pakiety mogą przychodzić szybciej niż odbiorca może je przetworzyć.

Protokół UDP

- Program użytkowy korzystający z UDP musi na siebie wziąć odpowiedzialność za rozwiązanie problemów niezawodności.
- Ponieważ sieci lokalne dają dużą niezawodność i małe opóźnienia wiele programów opartych na UDP dobrze pracuje w sieciach lokalnych, ale może zawodzić w większych intersieciach TCP/IP.

Protokół UDP

Format komunikatu UDP



Protokół UDP

Format komunikatu UDP

- Nagłówek datagramu użytkownika składa się z czterech 16-bitowych pól:
  - Pola PORT NADAWCY i PORT ODBIORCY zawierają 16-bitowe numery portów UDP używane do odnajdywania procesów oczekujących na dany datagram (pole PORT NADAWCY jest opcjonalne.

Protokół UDP

Format komunikatu UDP

- Pole DŁUGOŚĆ zawiera wartość odpowiadającą liczbie bajtów datagramu UDP wliczając nagłówek i dane (minimalnie 8, czyli jest długością samego nagłówka)
- Pole SUMA KONTROLNA jest opcjonalne. Ponieważ jednak IP nie wylicza sum kontrolnych dla danych, suma kontrolna UDP jest jedyną gwarancją, że dane nie zostały uszkodzone.

Protokół UDP

Kapsułkowanie UDP

- Datagram UDP jest kapsułkowany w datagram IP.
- Nagłówek IP identyfikuje maszynę źródłową i docelową, UDP - identyfikuje porty nadawcy i port odbiorcy.
- U odbiorcy pakiet dociera do najniższej warstwy oprogramowania sieciowego i wędruje ku coraz wyższym warstwom.
- Każda z nich usuwa jeden nagłówek, oczekujący proces otrzymuje więc komunikat bez nagłówków.

Multipleksowanie i demultipleksowanie

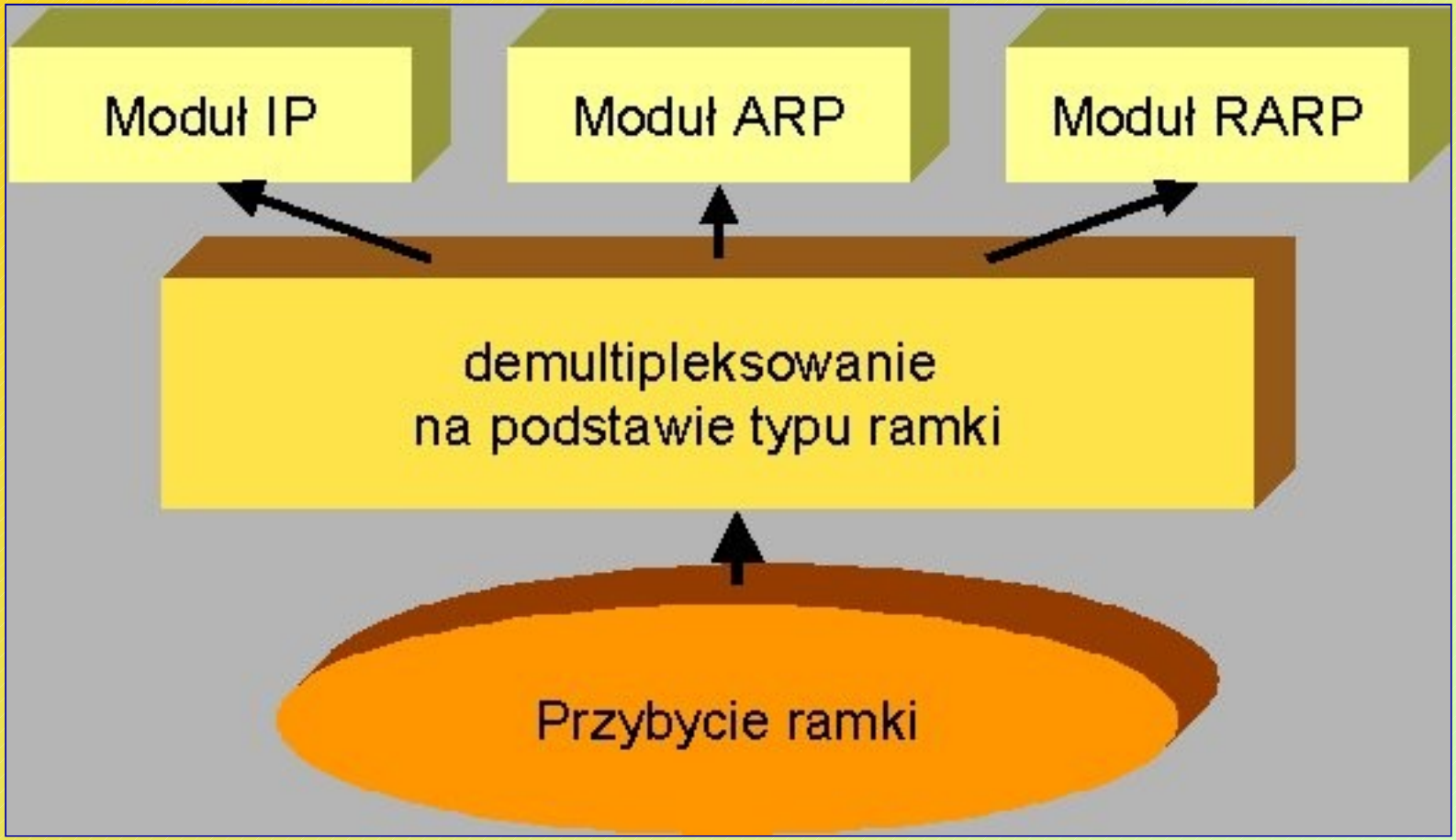
- Protokoły komunikacyjne wykorzystują metody multipleksowania i demultipleksowania na poziomach wszystkich warstw.
- Przy wysyłaniu komputer nadawcy dołącza do danych dodatkowe bity, które wskazują:
  - typ komunikatu,
  - program, który go nadał,
  - używane protokoły

Multipleksowanie i demultipleksowanie

- Wszystkie komunikaty są umieszczane w przeznaczonych do przesyłania ramkach sieciowych i łączone w strumień pakietów.
- U odbiorcy zaś te informacje są używane do sterowania przetwarzaniem.
- Multipleksowanie i demultipleksowanie pojawia się w prawie wszystkich warstwach protokołów.
- Aby zdecydować, w jaki sposób obsłużyć datagram, oprogramowanie sprawdza nagłówek datagramu i wybiera odpowiednie procedury.

Multipleksowanie i demultipleksowanie

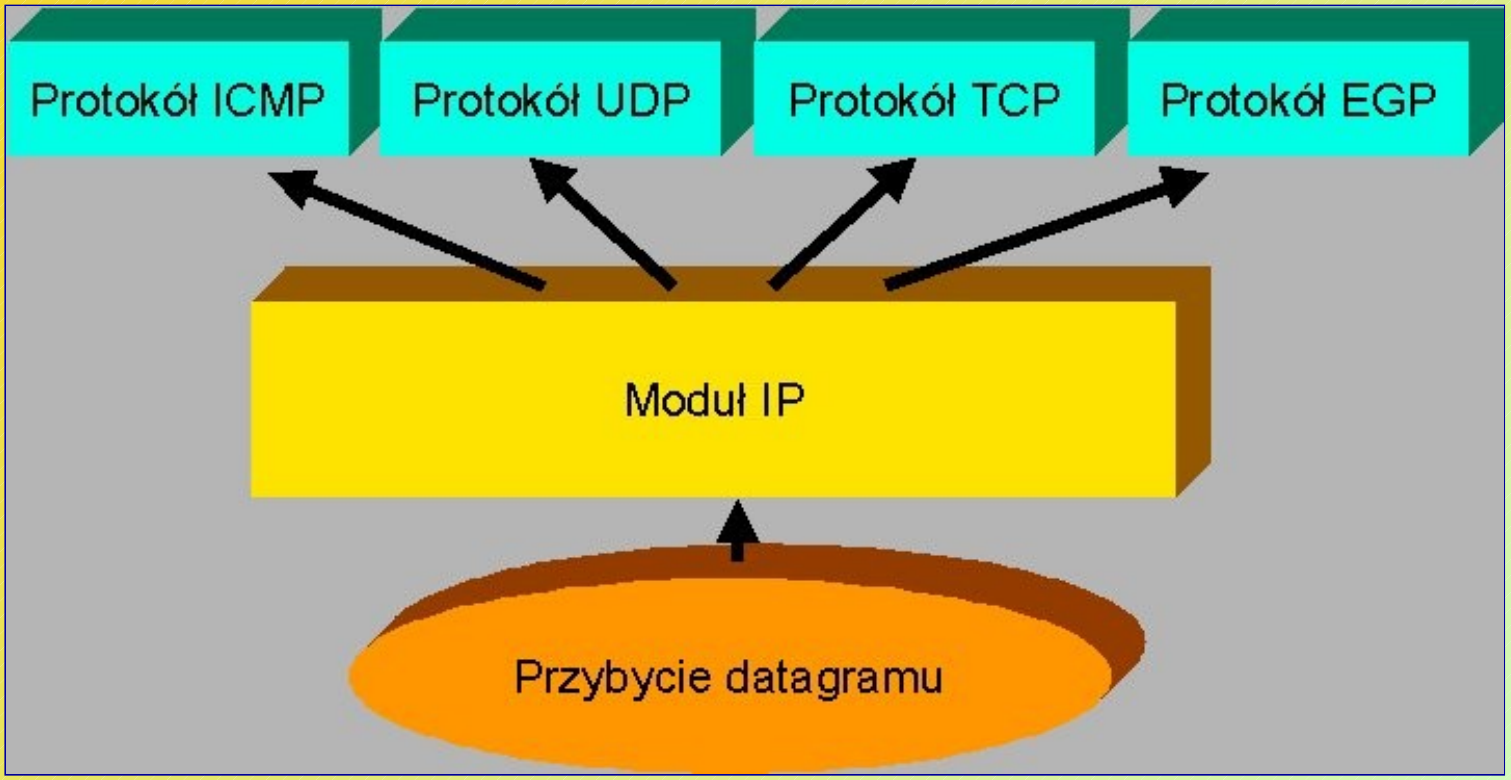
Demultipleksowanie na podstawie typu ramki



Multipleksowanie i demultipleksowanie

Demultipleksowanie w warstwie IP

- Oprogramowanie IP wybiera procedurę obsługi na podstawie pola typu protokołu.



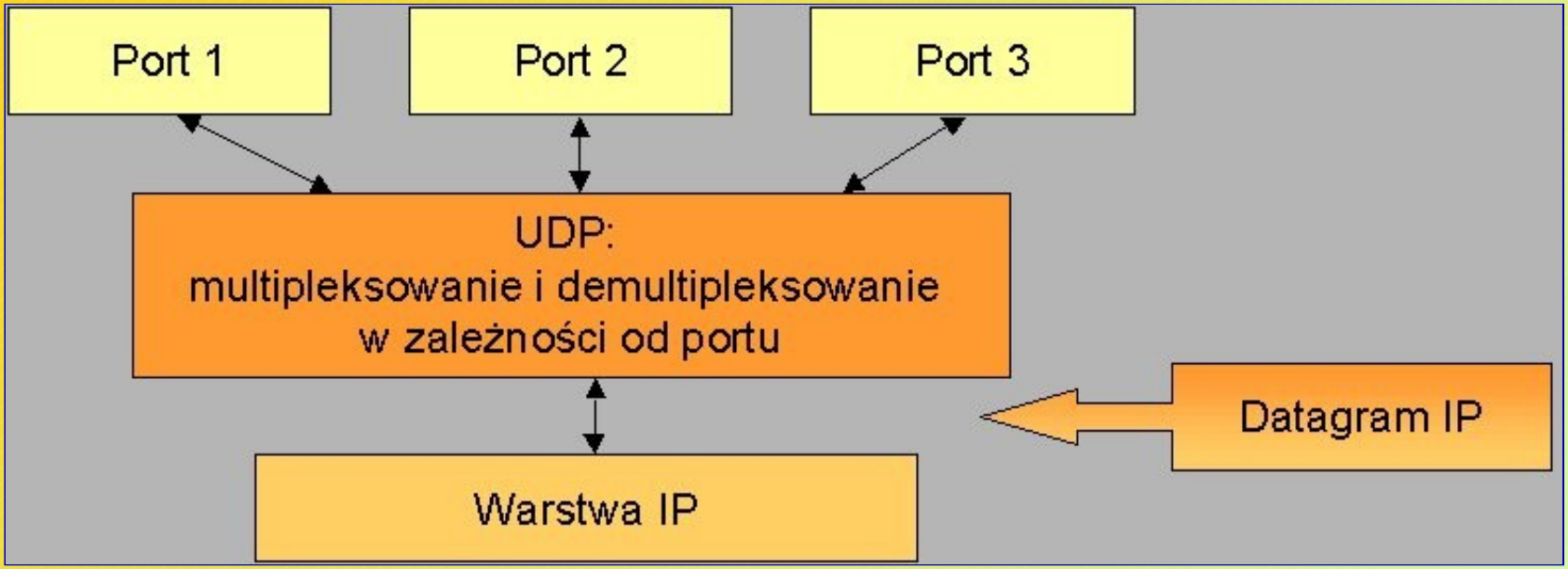
Multipleksowanie i demultipleksowanie

Demultipleksowanie UDP

- Oprogramowanie UDP przyjmuje datagramy UDP pochodzące od wielu programów użytkowych i przekazuje je warstwie IP.
- Aby to zrealizować musi multipleksować datagramy UDP tak aby datagramy pochodzące z różnych portów mogły być przekazane do warstwy IP i demultipleksować datagramy przychodzące z warstwy IP tak by skierować je do właściwego portu.

Multipleksowanie i demultipleksowanie

Demultipleksowanie UDP



Protokół TCP

- Protokoły warstwy czwartej:**TCP**: *Transmission Control Protocol*
- Wykorzystywany jest do transportu danych w trybie połączeniowym.
- Jego główną funkcją jest zarządzanie połączeniami między komputerami.
- Protokół ten zapewnia tzw. przesyłanie niezawodnymi strumieniami, które istotnie zwiększa funkcjonalność, biorąc odpowiedzialność za wiarygodne dostarczenie datagramu.

Protokół TCP

- TCP organizuje dwukierunkową współpracę między warstwą IP, a warstwami wyższymi, uwzględniając przy tym wszystkie aspekty priorytetów i bezpieczeństwa.
- Połączenia negocjowane są w trzyetapowym procesie i jeśli nie nastąpi przerwanie połączenia,

  to protokół utrzymuje je do końca transmisji.
- Komunikacja odbywa się w trzech fazach:
  - ustanowienie połączenia,
  - transfer danych,
  - rozłączenie połączenia.

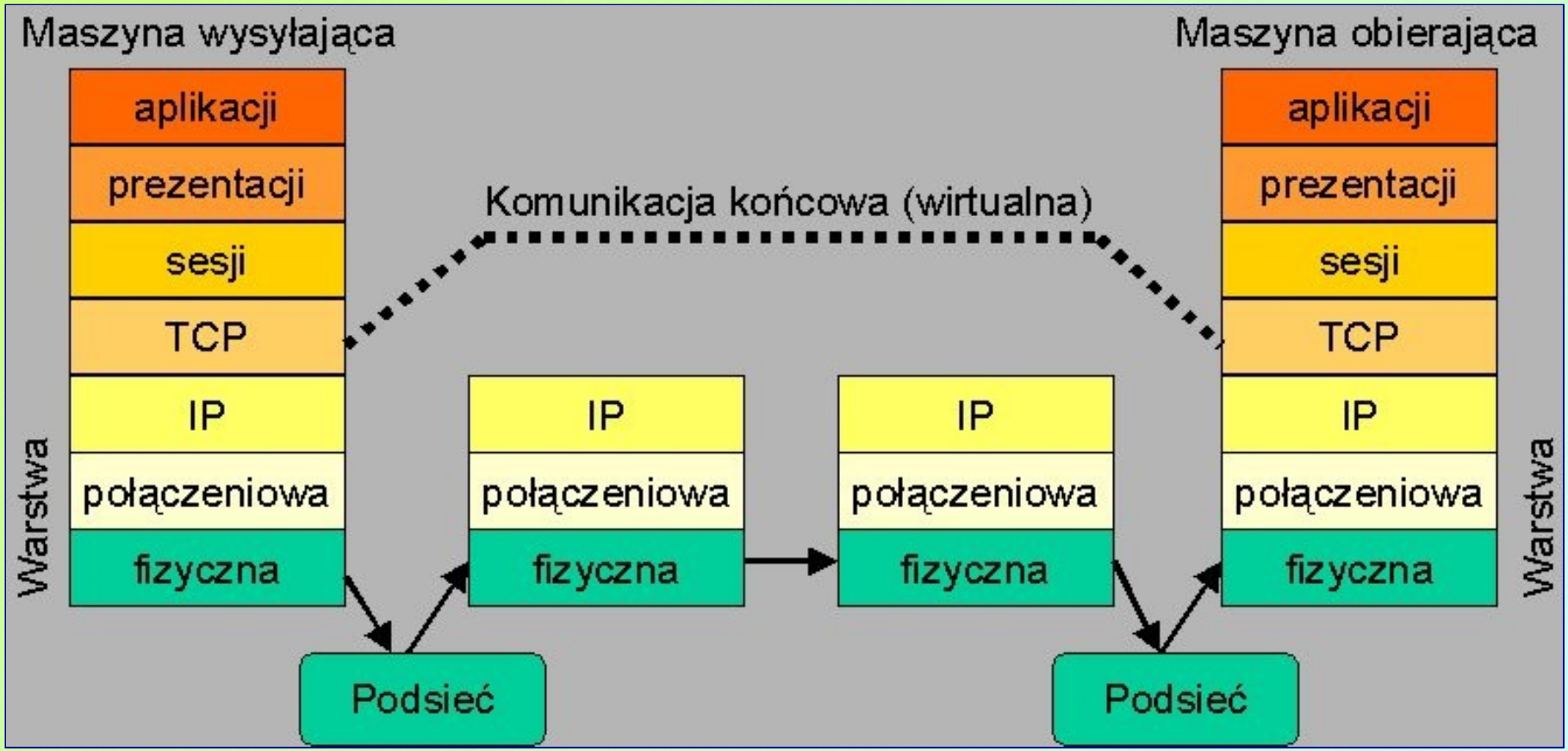
Protokół TCP

Kanał wirtualny TCP

- Rozpatrując TCP z punktu widzenia funkcjonalności można potraktować jego pracę jako ustanowienie kanału wirtualnego realizującego komunikację między "końcówkami" - tak wygląda to z punktu widzenia aplikacji użytkownika.
- Rzeczywisty przepływ odbywa się jednak poprzez warstwę IP i warstwy niższe.

Protokół TCP

Kanał wirtualny TCP



Protokół TCP

Realizacja niezawodnego połączenia

- Aby zagwarantować, że dane przesyłane z jednej maszyny do drugiej nie są ani tracone, ani duplikowane używa się podstawowej metody znanej jako pozytywne potwierdzanie z retransmisją.
- Metoda ta wymaga, aby odbiorca komunikował się z nadawcą, wysyłając mu w momencie otrzymania danych komunikat potwierdzenia (*ACK*).

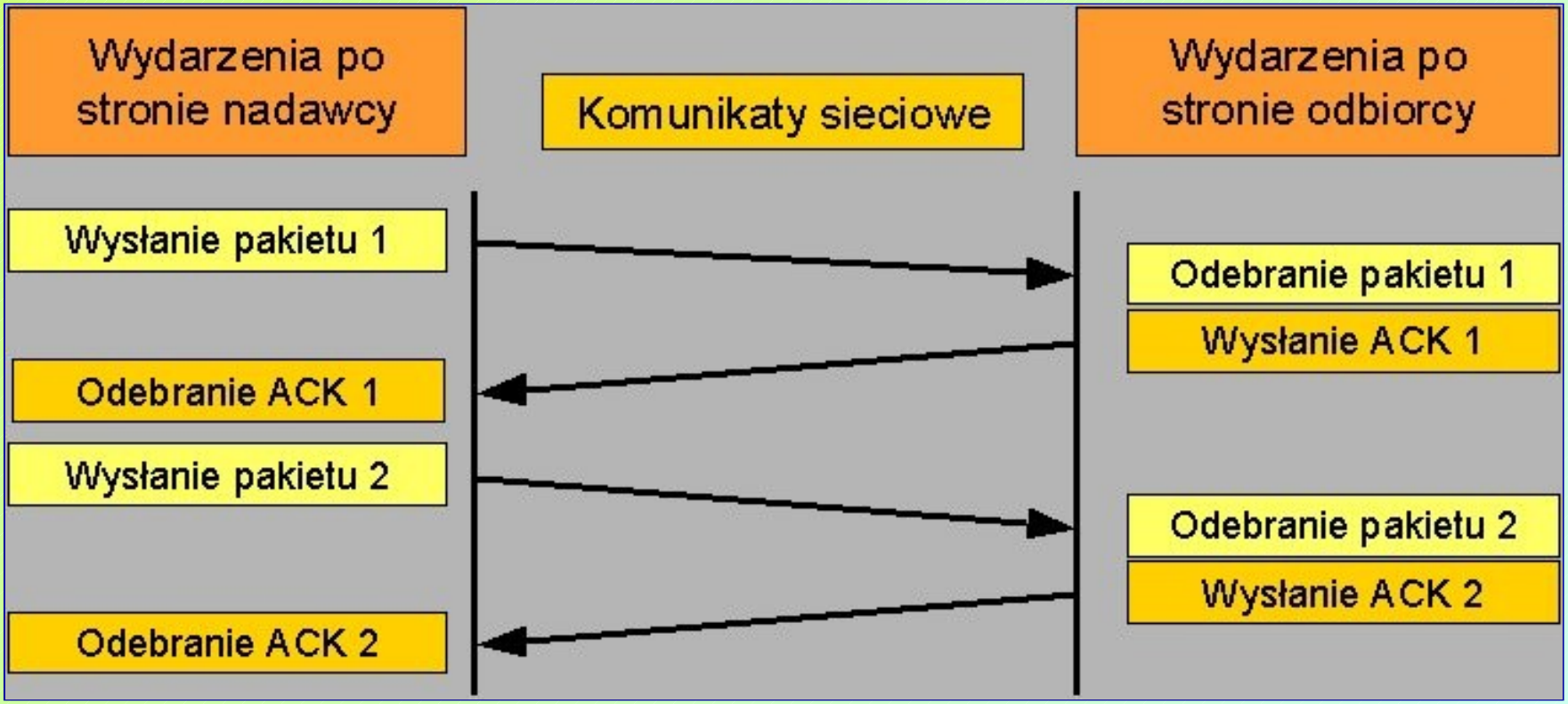
Protokół TCP

Realizacja niezawodnego połączenia

- Nadawca przechowuje informację o każdym wysłanym pakiecie i przed wysłaniem następnego czeka na potwierdzenie.
- Oprócz tego nadawca uruchamia zegar w momencie wysyłania pakietu i wysyła ten pakiet ponownie, gdy minie odpowiedni czas, a potwierdzenie nie nadejdzie.

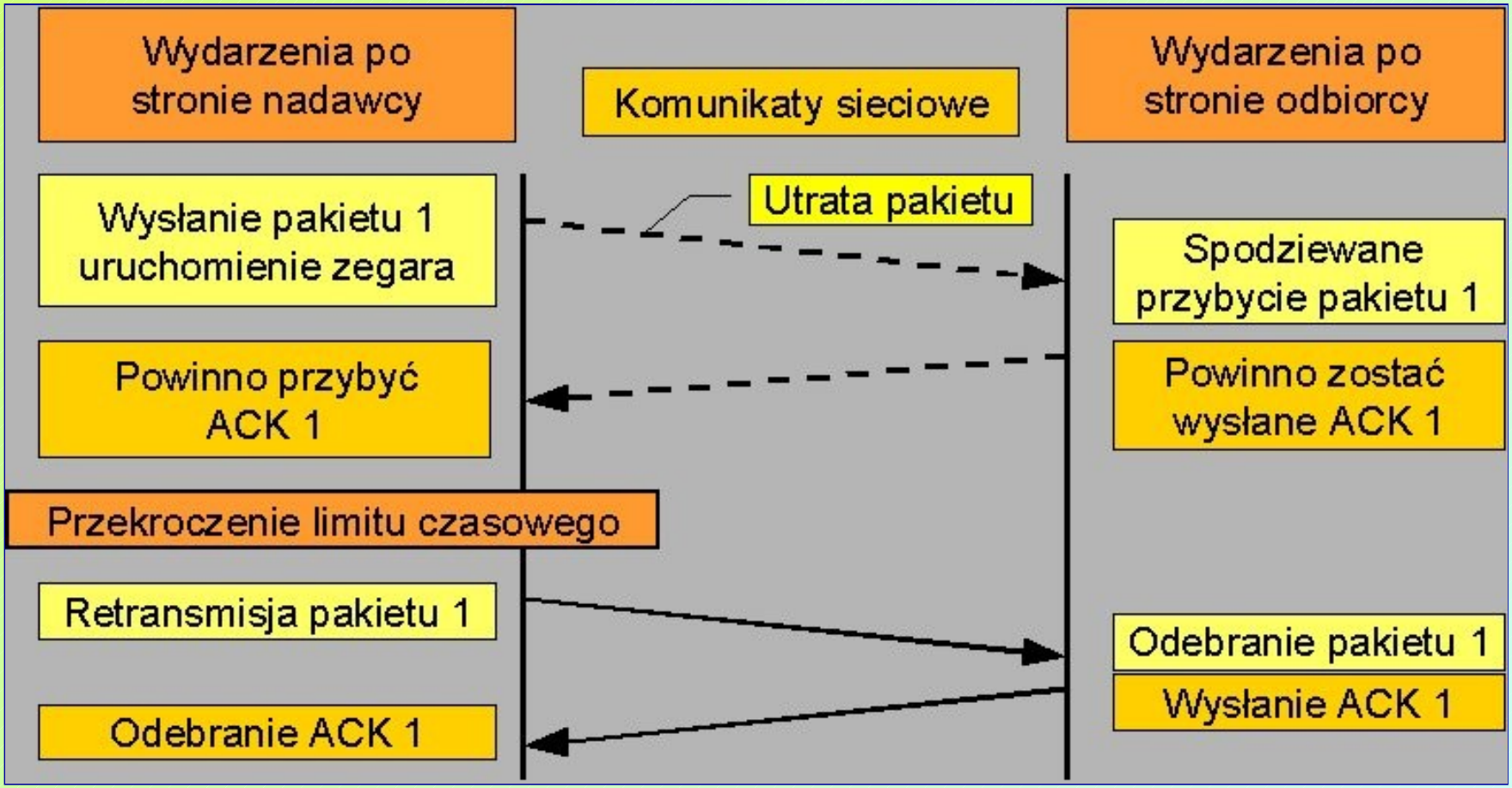
Protokół TCP

Realizacja niezawodnego połączenia



Protokół TCP

Realizacja niezawodnego połączenia



Protokół TCP

Idea przesuwających się okien

- W celu uzyskania niezawodności nadawca wysyła pakiet, a przed wysłaniem następnego oczekuje na potwierdzenie odebrania.
- Dane w danym momencie płyną tylko w jednym kierunku i to nawet wtedy, kiedy sieć umożliwia jednoczesną komunikację w obu kierunkach.
- Ponadto sieć nie będzie używana, kiedy maszyny będą zwlekać z odpowiedziami np. podczas wyliczania sum kontrolnych - takie rozwiązanie powoduje marnowanie przepustowości sieci.

Protokół TCP

Idea przesuwających się okien

- Technika przesuwającego się okna lepiej wykorzystuje przepustowość sieci, gdyż umożliwia wysyłanie wielu pakietów przed otrzymaniem potwierdzenia.
- W rozwiązaniu tym umieszcza się na ciągu pakietów ustalonego rozmiaru okna i przesyła wszystkie pakiety, które znajdują się w obrębie takiego okna.

Protokół TCP

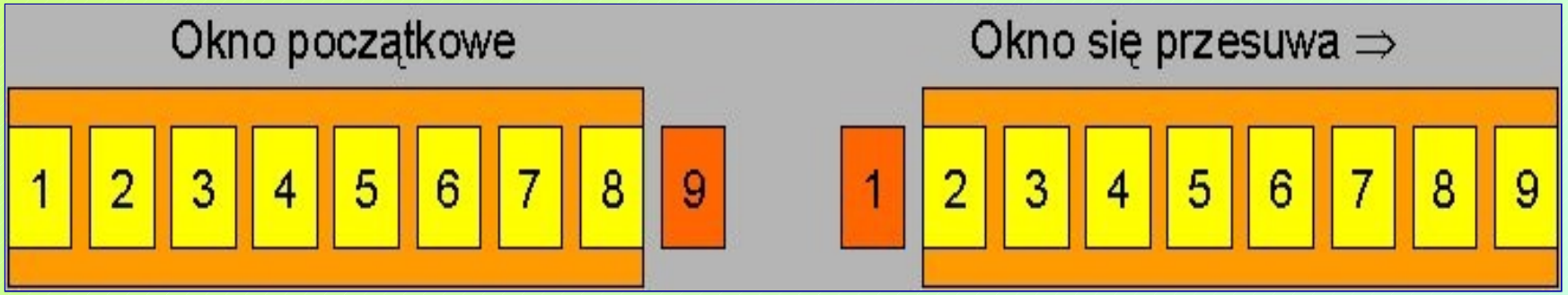
Idea przesuwających się okien

- Pakiet jest niepotwierdzony, jeżeli został wysłany, a nie nadeszło dla niego potwierdzenie.
- Liczba pakietów niepotwierdzonych w danej chwili jest wyznaczona przez rozmiar okna.
- Dla protokołu z przesuwającym się oknem , którego rozmiar jest np. równy 8, nadawca ma możliwość wysłania przed otrzymaniem potwierdzenia do 8 pakietów.
- Gdy nadawca odbierze potwierdzenie dla pierwszego pakietu, okno przesuwa się i zostaje wysłany następny pakiet.

Protokół TCP

Idea przesuwających się okien

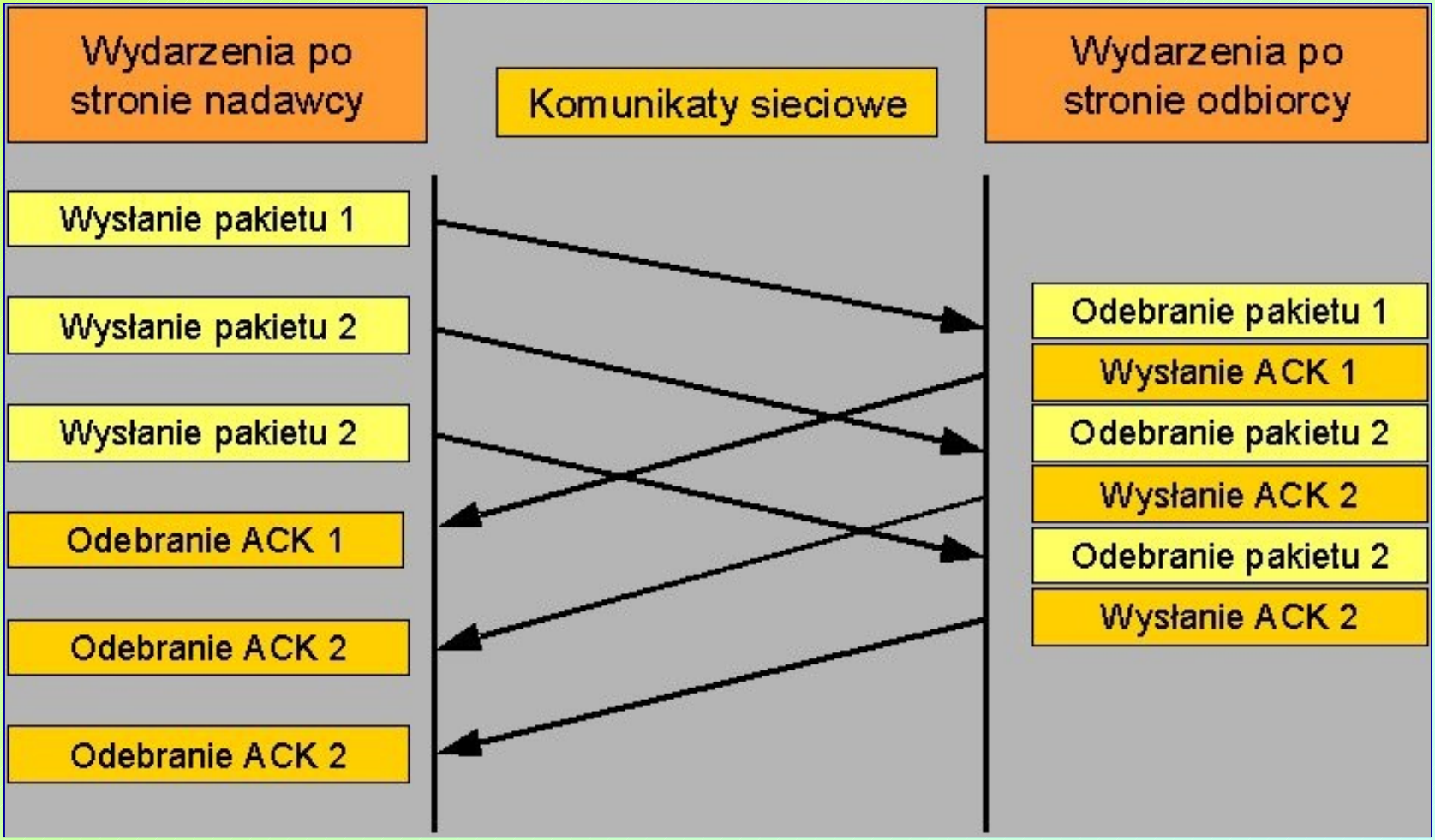
- Okno przesuwa się dalej gdy przychodzą kolejne potwierdzenia.



- Pakiet 9-ty może zostać wysłany gdy przyszło potwierdzenie dotyczące pierwszego pakietu.
- Retransmitowane są tylko te pakiety, dla których nie było potwierdzenia.

Protokół TCP

Idea przesuwających się okien



Protokół TCP

Segment TCP

- Jednostkowa porcja danych przesyłanych między oprogramowaniem TCP na różnych maszynach.

Protokół TCP

Segment TCP – opis pól

- Pola PORT NADAWCY i PORT ODBIORCY zawierają numery portów TCP, które identyfikują programy użytkowe na końcach połączenia.
- Pole NUMER PORZĄDKOWY wyznacza pozycję danych segmentu w strumieniu bajtów nadawcy.
- Pole NUMER POTWIERDZENIA wyznacza numer oktetu, który nadawca spodziewa się otrzymać w następnej kolejności.

Protokół TCP

Segment TCP – opis pól

- Pole DŁUGOŚĆ NAGŁÓWKA zawiera liczbę całkowitą, która określa długość nagłówka segmentu mierzoną krotnością 32 bitów.
- Pole ZAREZERWOWANE jest pozostawione do wykorzystania w przyszłości.
- Pole BITY KODU zawiera informację o przeznaczeniu zawartości segmentu (dane, potwierdzenie, prośba o ustanowienie lub zamknięcie połączenia).
- Pole OKNO - określa maksymalny rozmiar danych które można umieścić w segmencie.

Protokół TCP

Porty i połaczenia

- Protokół TCP umożliwia wielu działającym na jednej maszynie programom użytkowym jednoczesne komunikowanie się oraz rozdziela między te programy przybywające pakiety TCP.
- TCP używa numerów portów protokołu do identyfikacji w ramach maszyny końcowego odbiorcy.
- Każdy z portów ma przypisaną małą liczbę całkowitą, która jest używana do jego identyfikacji.

Protokół TCP

Porty i połaczenia

- Porty TCP są jednak bardziej złożone, gdyż dany numer nie odpowiada bezpośrednio pojedynczemu obiektowi.
- TCP działa wykorzystując połączenia, w których obiektami są obwody wirtualne a nie poszczególne porty.
- Tak więc podstawowym pojęciem TCP jest pojęcie połączenia, a nie portu.
- Połączenia są identyfikowane przez parę punktów końcowych.

Protokół TCP

Porty i połaczenia

- TCP definiuje punkt końcowy jako parę liczb całkowitych (węzeł, port), gdzie
  - węzeł oznacza adres IP węzła,
  - a port jest portem TCP w tym węźle.
- W związku z tym, że TCP identyfikuje połączenie za pomocą pary punktów końcowych, dany numer portu może być przypisany do wielu połączeń na danej maszynie.

Protokół TCP

Porty i połaczenia - przykład

- Punkt końcowy (128.10.2.3, 25) oznacza port 25 maszyny o adresie IP 128.10.2.3.
- W efekcie może istnieć połączenie np. pomiędzy:

  (18.26.0.36, 1069) oraz (128.10.2.3, 25),

  w tym samym czasie może też istnieć połączenie

  (128.9.0.32, 1184) oraz (128.10.2.3, 25).

Protokół TCP

Konfiguracja TCP/IP w UNIX-ie

- Konfiguracja większości wersji systemu UNIX, opiera się na kilku plikach konfiguracyjnych wymienionych w tabeli.
- W niektórych implementacjach pliki mogą się różnić nazwami, lecz ich znaczenie pozostaje takie samo.
- Wymienione pliki są plikami tekstowymi, więc do ich modyfikacji potrzebny jest dowolny edytor tekstowy, operujący w czystym kodzie ASCII.

Protokół TCP

Konfiguracja TCP/IP w UNIX-ie

Nazwa pliku	Znaczenie
/etc/hosts	Nazwy maszyn w sieci (hostów)
/etc/networks	Mnemoniczne nazwy sieci
/etc/services	Lista dostępnych usług
/etc/protocols	Lista protokołów
/etc/hosts.equiv	Lista zaufanych hostów (ang. trusted hosts)
/etc/inetd.conf	Lista serwerów uruchamiających program inetd

Przyszłość TCP/IP

- Gdy powstawała wersja 4 protokołu IP, 32-bitowy adres wydawał się wystarczający na długie lata rozwoju Internetu; wyczerpanie się adresów (jest ich teoretycznie 2^{32}, w praktyce mniej z uwagi na sposób adresowania, istnienie adresów grupowych i zarezerwowanych) traktowano jako coś zupełnie niemożliwego.
- Rzeczywistość szybko przerosła jednak wyobraźnię - Internet rozrasta się w postępie geometrycznym, a ilość przyłączonych hostów podwaja się z każdym rokiem.

Przyszłość TCP/IP

- W związku z tym pojawiło się kilka propozycji rozwiązania tego problemu.
- Zaowocowały one pewnym kompromisem będącym punktem wyjścia dla opracowania kolejnej wersji protokołu IP.
- Wersja ta znana jest pod roboczą nazwą IP Next Generation (*IPng*) lub IP wersja 6 i znajduje się obecnie w zaawansowanym stadium eksperymentów.

IP Next Generation

- Nowy, 128-bitowy system adresowania.
- Udoskonalona postać nagłówka IP z rozszerzeniami dla aplikacji i opcji
- Brak sumy kontrolnej
- Nowe pole kontrolne zwane etykietą potoku
- Zabezpieczenie przed zjawiskiem tzw. fragmentacji pośredniej.
- Wbudowane narzędzia kryptograficzne i mechanizmy weryfikacji .