Sieci komputerowe:

NIŻSZE WARSTWY MODELU OSI

Agata Półrola

Katedra Informatyki Stosowanej UŁ

polrola@math.uni.lodz.pl

http://www.math.uni.lodz.pl/~polrola

Literatura

- D. Comer: *Sieci komputerowe TCP/IP,* tom 1, WNT
- *D. Comer: Sieci komputerowe i intersieci*, WNT
- L. L. Peterson: *Computer Networks. A System Approach*
- A. Frisch: *Unix. Administracja systemu*, O'Reilly & ReadMe
- C. Hunt: *TCP/IP. Administracja sieci.* O'Reilly & ReadMe

Głównym celem tworzenia sieci jest możliwość korzystania np. ze wspólnych urządzeń peryferyjnych czy zasobów dyskowych

Praca w sieci (ang. *networking*) – współdzielenie informacji i usług

Historia

- 1969 – pierwsze fragmenty sieci ARPANET (USA)
- ok. 1980 – początki światowego Internetu
- 1983 – wyodrębnienie z sieci ARPANET sieci MILNET (do zastosowań wojskowych)

Modele pracy w sieci

Klasyfikacja ze wzgl. na sposób przetwarzania:

- przetwarzanie scentralizowane *(centralized computing)*
- przetwarzanie rozproszone *(distributed computing)*
- przetwarzanie wspólne *(collaborative computing)*

Klasyfikacja ze wzgl. na sposób udostępniania usług:

- klient – serwer
- klient - sieć

Przetwarzanie scentralizowane

- Do przetwarzania i przechowywania danych służą komputery centralne (ang. *mainframes*)
- wprowadzanie danych odbywa się za pośrednictwem terminali
- sieć umożliwia współdzielenie informacji i usług przez komputery centralne

Przetwarzanie rozproszone

- wszystkie komputery mają zdolność przetwarzania danych
- wykonywane zadanie jest dzielone na podzadania przydzielane poszczególnym komputerom
- wyniki podzadań przesyłane są innym komputerom (komunikacja za pośrednictwem sieci)

Przetwarzanie wspólne

- odmiana przetwarzania rozproszonego
- komputery współdzielą zdolność przetwarzania danych (jeden komputer może korzystać z zasobów innego)
- jedno (pod)zadanie może być przetwarzane przez kilka komputerów

Model klient - serwer

- wielu klientów jest połączonych z jednym lub wieloma serwerami
- wiele maszyn ma zdolność przetwarzania danych
- klienci korzystają z usług udostępnianych przez serwery
- serwery wykonują pewne działania (przetwarzanie danych) dla klientów

Aplikacje działające w sieci klient – serwer można podzielić na tzw. *front-end* (uruchamiane u klienta) i *back-end* (uruchamiane na serwerze)

Model klient - sieć

- Użytkownicy logując się do sieci uzyskują dostęp do zbioru usług, a nie do konkretnych serwerów
- usługi mogą być udostępniane np. za pomocą tzw. usług katalogowych, jak np. NDS – *Novell Directory Service*

Klasyfikacja sieci ze względu na zasięg

- sieci lokalne - LAN (*Local Area Networks*)
- sieci MAN *(Metropolitan Area Networks*),
- sieci o szerokim zasięgu - WAN (*Wide Area Networks*)
- sieć globalna

Klasyfikacja sieci ze względu na sposób organizacji

- sieci „każdy z każdym” *(peer-to-peer)*
- sieci z centralnym serwerem *(server-centric)*

  - klient – korzysta z usług
  - serwer – udostępnia usługi
  - *peer* – zarówno udostępnia usługi, jak i z nich korzysta

Klasyfikacja sieci ze wzgl. na sposób komunikacji

- sieci z komutacją obwodów (zorientowane połączeniowo) (ang. *connection-oriented, circuit-switched*)
  - zasada działania: tworzenie dedykowanych połączeń między elementami sieci
  - zaleta: gwarantowana przepustowość łącza
  - wada: stały koszt połączenia niezależnie od ilości przesłanych danych
- sieci z komutacją pakietów (bezpołączeniowe) (ang. *packet-switched, connectionless*)
  - dane do przesłania dzielone są na małe porcje (komunikaty, pakiety – ang. *messages, packets*)
  - zaleta: współdzielenie łącza
  - wada: przeciążenia

Elementy sieci

Sieć wymaga następujących elementów:

- usług sieciowych (zapotrzebowania na współdzielenie pewnych zasobów)
  - może być z nimi związany sieciowy system operacyjny
- medium transmisyjnego (umożliwiającego komunikowanie się)
- protokołów (zasad komunikacji)

Usługi sieciowe

- usługi plikowe *(file services)*
- usługi drukowania *(print services)*
- usługi informacyjne *(information services)*
- usługi aplikacyjne *(application services)*
- usługi bazodanowe *(database services)*

Sieciowe systemy operacyjne

Wykonanie zadania przez program komputerowy wymaga zazwyczaj pewnej kombinacji danych, zasobów urządzeń wejścia/wyjścia oraz mocy obliczeniowej. Usługi sieciowe umożliwiają komputerom współdzielenie ich zasobów przy użyciu specjalnych aplikacji sieciowych. Aplikacje udostępniające zasoby sieciowe mogą być połączone w jeden sieciowy system operacyjny.

Sieciowe systemy operacyjne koordynują i udostępniają różne zasoby sieciowe innym programom komputerowym.

Sieciowy system operacyjny – wyspecjalizowany system operacyjny, który zarządza zasobami wykorzystywanymi przez wielu klientów, koordynując współdzielenie przez nich usług sieciowych.

Przykłady:

- Banyan Vines, Novell NetWare, Open VMS (server-centric)
- Windows NT, Windows for Workgroups, Windows XP (peer-to-peer)

Media transmisyjne

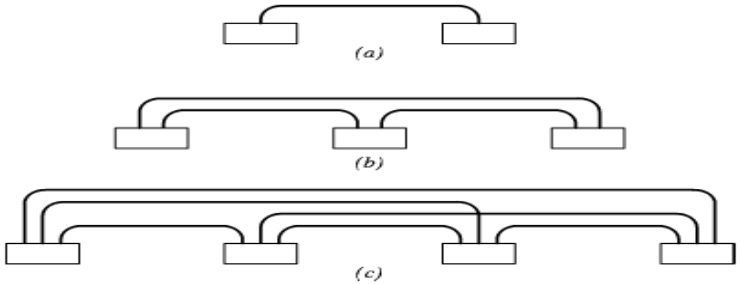
Media transmisyjne – technologie bezprzewodowe i przewodowe pozwalające na komunikację między urządzeniami dołączonymi do sieci

Media transmisyjne nie gwarantują, że komunikat przesłany siecią zostanie zrozumiany przez komputer – odbiorcę. Stanowią jedynie drogę dostarczenia komunikatu.

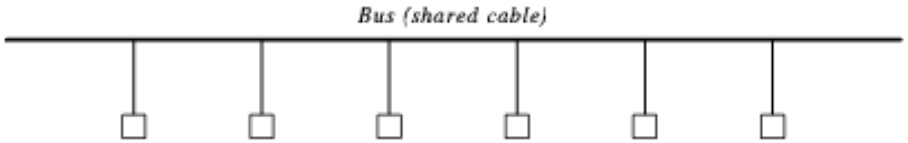
- połączenie fizyczne – *łącze (ang. link)*
- połączone komputery – *węzły, hosty (ang. nodes, hosts)*

Typy połączeń

- każdy z każdym *(point-to-point)*



- łącze wielodostępne *(multiple-access link)*

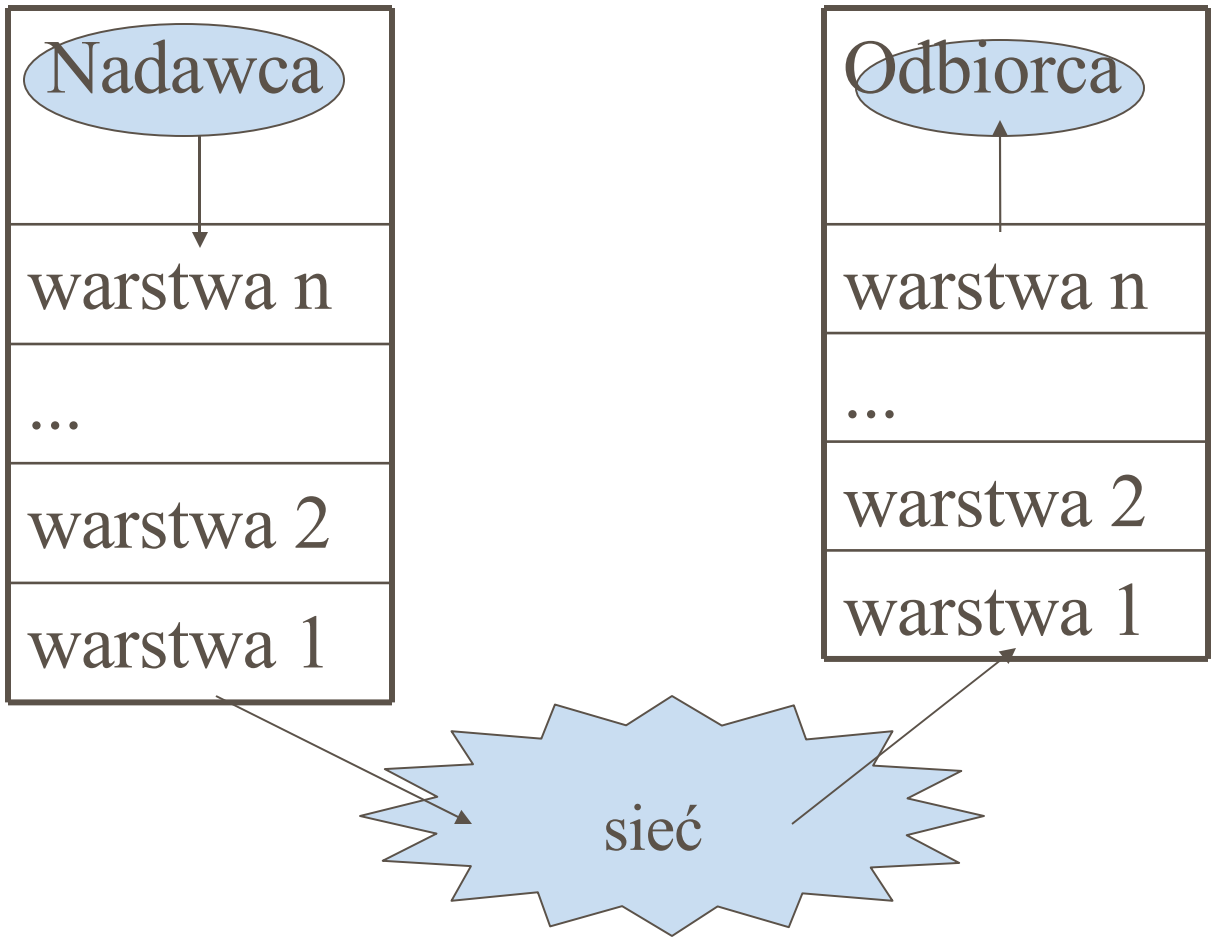


Protokoły

- Protokoły określają zasady komunikacji i umożliwiają wzajemne „rozumienie się” urządzeń dołączonych do sieci
- Protokół może być pojedynczą regułą albo zbiorem reguł lub standardów pozwalających na komunikację różnych urządzeń
- Protokoły umożliwiają komunikację bez znajomości szczegółów sprzętu sieciowego

Złożone systemy komunikacyjne wymagają zazwyczaj zbiorów współpracujących protokołów (są to tzw. rodziny protokołów – *protocol families, protocol suites*), a nie pojedynczego protokołu

Warstwy protokołów



Model warstwowy ISO / OSI

7	warstwa aplikacji
6	warstwa prezentacji
5	warstwa sesji
4	warstwa transportu
3	warstwa sieci
2	warstwa łącza danych
1	warstwa fizyczna

Warstwy modelu OSI:

- warstwa aplikacji - zawiera programy aplikacyjne korzystające z sieci (programy transferu plików, programy pocztowe itp.)
- warstwa prezentacji - opisuje reprezentację danych, zawiera funkcje wykorzystywane przez wiele programów korzystających z sieci (np. standardowe metody kompresji tekstu lub konwersji grafiki do postaci strumienia bitów, w jakiej mają być transmitowane przez sieć)
- warstwa sesji – obsługa dostępu zdalnego (bezpieczeństwo, identyfikacja za pomocą haseł itp.)
- warstwa transportowa – zapewnia niezawodny przesył danych

- warstwa sieci – definiuje podstawową jednostkę transferu danych w sieci (tzw. datagram), adresowanie i trasowanie; obsługuje przeciążenia sieci i zgodność rozmiaru datagramów z rozmiarem ramek sieci fizycznej
- warstwa łącza danych – określa sposób przesyłania danych w sieci, definiuje podstawową jednostkę przesyłu (ramkę sieci fizycznej), sposób rozpoznawania granic ramki przez urządzenia, definiuje sposób wykrywania błędów (sumy kontrolne ramek) oraz sposób wymiany komunikatów pozwalających maszynom „wiedzieć” że ramka została przesłana poprawnie
- warstwa fizyczna – określa standardy połączeń fizycznych między urządzeniami sieciowymi (w tym np. charakterystykę elektryczną) oraz procedury użuwane do przesyłania danych między urządzeniami

Model warstwowy TCP/IP

4	warstwa aplikacji
3	warstwa transportu
2	warstwa internetu
1	warstwa interfejsu sieciowego
0	*sprzęt*

Warstwy modelu TCP/IP

- warstwa aplikacji – programy użytkowe korzystające z usług dostępnych w sieci TCP/IP; komunikują się one z którymś z protokołów warstwy transportu. Wybierają sposób transferu danych (sekwencja pojedynczych komunikatów, ciągły strumień bajtów) i przekazują dane w odpowiedniej postaci do protokołu warstwy transportu
- warstwa transportu – zapewnia komunikację między aplikacjami (*end-to-end communnication*); może regulować przepływ danych, zapewnia niezawodny transport; dokonuje podziału danych w strumieniu na mniejsze części (pakiety) i przekazuje je niższej warstwie do przesyłu

- warstwa intersieci – zapewnia komunikację między maszynami; wykonuje kapsułkowanie pakietów w datagramy IP, określa nagłówki datagramów i podejmuje decyzję czy datagram ma być przesłany bezpośrednio do adresata, czy też do routera pośredniczącego (dokonuje wyboru trasy). Obsługuje datagramy przychodzące, sprawdza ich poprawność, przesyła komunikaty kontrolne
- warstwa interfejsu sieciowego – odpowiada za przesyłanie datagramów IP konkretną siecią fizyczną.

Warstwa fizyczna

technologie i topologie sieciowe

Media transmisyjne

Do przesyłania sygnałów między komputerami wykorzystuje się prąd elektryczny, mikrofale, fale świetlne lub radiowe.

Media transmisyjne można podzielić na przewodowe i bezprzewodowe.

Cechy mediów transmisyjnych:

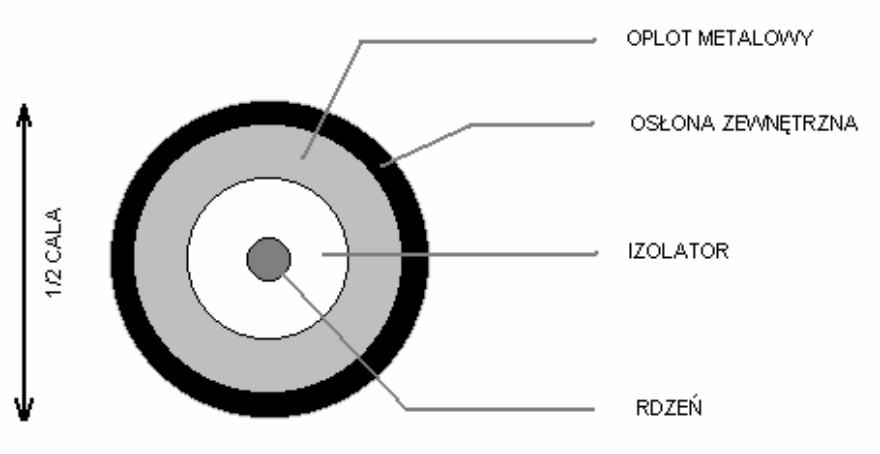
- koszt
- łatwość instalacji
- pojemność (przepustowość i szerokość pasma)
- tłumienie
- wrażliwość na zakłócenia i przechwycenie sygnału

- Przepustowość łącza dana jest przez liczbę bitów, jaka może być przesłana siecią w pewnym czasie (np. 10 Mbps – megabitów na sekundę).
  Inaczej – ile czasu wymaga przesłanie jednego bitu (tu: 0,1 μs)
- Opóźnienie określa, ile czasu zajmuje przesłanie jednego bitu z jednego końca łącza na drugi
  (czasami za bardziej istotny parametr uznaje się tzw. RTT – *round-trip time*)
- Tłumienie określa tendencję fal elektromagnetycznych do osłabiania się podczas przesyłu
- Zakłócenia mają miejsce w przypadku, gdy niepożądane fale elektromagnetyczne oddziałują na fale pożądane
- Przechwycenie sygnału – niektóre z transmitowanych fal elektromagnetycznych mogą być łatwo przechwycone, co pozwala skopiować przesyłane dane

Łącza fizyczne

- kabel koncentryczny
- skrętka telefoniczna
- włókna światłowodowe
- fale radiowe
- mikrofale
- promieniowanie podczerwone
- łącza satelitarne

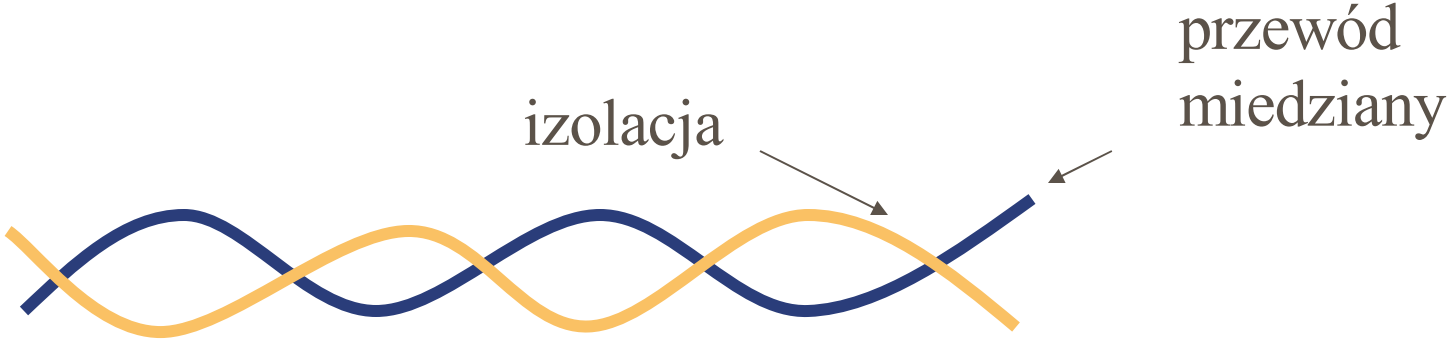
Kabel koncentryczny



kabel koncentryczny (Ethernet, *coaxial cable, coax):*

- przesył danych za pomocą sygnałów elektrycznych
- rdzeń zapewnia przewodzenie sygnału
- oplot metalowy (tzw. *ekran*) zapobiega przed promieniowaniem zewnętrznym oraz wypromieniowaniu na zewnątrz

Skrętka telefoniczna



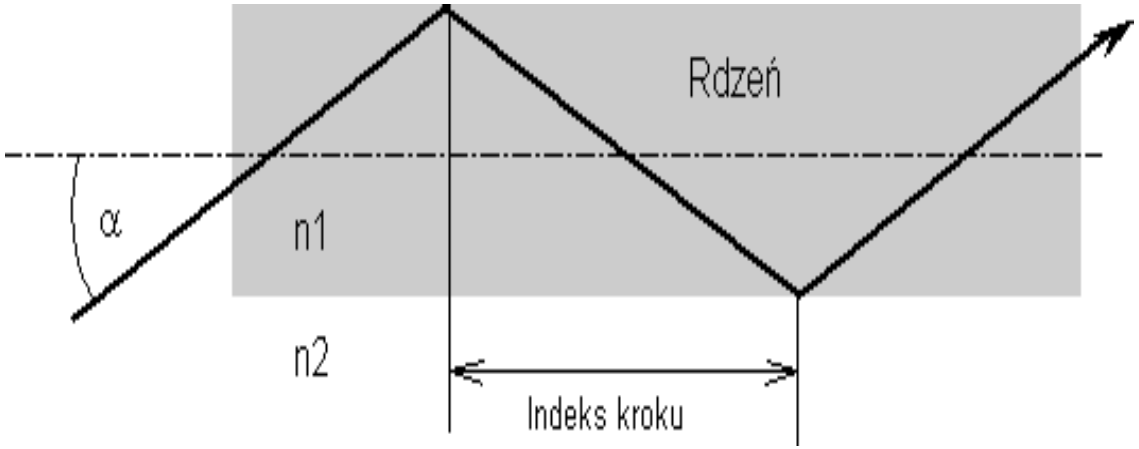
- Skrętka telefoniczna (*twisted pair):*
  - ekranowana *(shielded)* – STP
  - nieekranowana *(unshielded)* – UTP
- Skręcenie i ekranowanie kabli ma na celu zmniejszenie interferencji (unikanie zakłóceń)
- Dane przesyłane jako sygnał elektryczny

Włókna światłowodowe

- cienkie włókno szklane w plastikowej osłonie (zapobiega łamaniu, umożliwia zginanie)
- Przesyłanie danych:
  - na jednym końcu przewodu znajduje się dioda świecąca lub laser, służące do generowania sygnałów świetlnych przesyłanych włóknem;
  - na drugim końcu znajduje się odbiornik używający światłoczułego tranzystora wykrywającego te impulsy

Włókna światłowodowe – cd.

- ang. *fiber optic cables*
  - wielomodowe *(multimode fibers)* – 2 km
  - jednomodowe *(single-mode fibers)* – 40 km



Fale radiowe

- Nie jest wymagane bezpośrednie fizyczne połączenie komputerów, ale każdy komputer musi być podłączony do anteny, która nadaje i odbiera fale
- tego rodzaju transmisja może być podatna na przechwycenie sygnału

wykorzystywane m.in. w Bluetooth, Wi-Fi

Mikrofale

- Promieniowanie elektromagnetyczne o częstotliwości spoza zakresu wykorzystywanego przez radio i TV
- Można ukierunkować transmisję, co zabezpiecza przed odebraniem sygnału przez innych
- Mogą źle przechodzić np. przez struktury metalowe

Podczerwień

- transmisja ograniczona do małej przestrzeni oraz wymagająca, aby nadajnik był ukierunkowany na odbiornik
- przydatne w komputerach przenośnych (IRDA)
- umożliwia także stworzenie małej sieci komputerowej, np. w obrębie pomieszczenia

Łącza satelitarne

- Fale radiowe nie mogą pokonać krzywizny Ziemi, stąd wykorzystanie transmisji satelitarnej
- Satelita wyposażony jest w *transponder* odbierający sygnały radiowe i wysyłający je w kierunku Ziemi pod nieco zmienionym kątem. Zazwyczaj satelita ma wiele transponderów obsługujących różne długości fali, a z każdego może korzystać wielu użytkowników

Sygnał

- Każde medium używane jest do transmisji *sygnału*
- Sygnał może być cyfrowy (ang. *digital,* przyjmujący wartości dyskretne, np. napięcie + i -) lub analogowy (ang. *analog*, ciągły sygnał elektromagnetyczny zmieniający częstotliwość)
- Dane do przesłania muszą zostać zakodowane w postaci sygnału

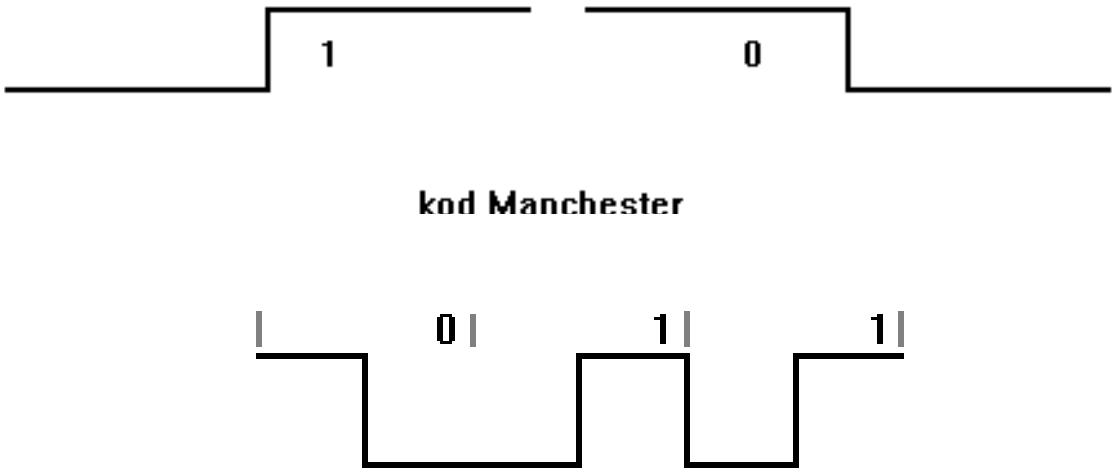
Kodowanie danych

- Modem (modulator/demodulator) jest urządzeniem kodującym dane binarne w sygnał analogowy po stronie transmitującej, a sygnał analogowy z powrotem na dane binarne po stronie odbierającej
- Karta sieciowa (*network adapter*) wyposażona jest w komponent odpowiadający za kodowanie danych binarnych do postaci możliwej do przesłania łączem cyfrowym oraz za rozkodowywanie otrzymanego sygnału

Sposoby kodowania sygnału

- kod NRZ (*non-return-to-zero*)
  - 1 – sygnał „wysoki”, 0 – „niski”
- kod NRZI (*non-return-to-zero inversed*)
  - 1 - dowolne przejście między sygnałem „wysokim” i „niskim”, 0 – brak zmiany wysokości
- kod Manchester
  - 1 – przejście z sygnału „niskiego” do „wysokiego”, 0 - przejście z sygnału „wysokiego” do „niskiego”
- 4B/5B – wstawianie w (trudne do zakodowania) długie sekwencje zer lub jedynek dodatkowego bitu przerywającego te sekwencje

Kod Manchester



Rodzaje transmisji

- Jedną z cech łącza jest, ile strumieni bitów może być w nim zakodowanych równocześnie
  - jeśli jeden, to węzły sieci muszą dzielić dostęp do łącza
  - jedną z częstych cech łączy *point-to-point* jest, że dwa strumienie bitów mogą być nimi transmitowane równocześnie w przeciwne strony. Jest to tzw. pełny dupleks *(full duplex link)*. Jeśli możliwa jest tylko transmisja w jedną stronę, to użytkownicy muszą korzystać z łącza na przemian (półdupleks, ang. *half-duplex*)

Identyfikacja urządzenia w sieci fizycznej

- W sieciach o wspólnym medium sygnał wysyłany przez jedną stację dociera do wszystkich innych. Interfejs sieciowy każdej stacji odbiera sygnał i odczytuje przesłaną ramkę
- Adresy sprzętowe (adresy fizyczne, MAC adresy) identyfikują interfejs sieciowy w sieci fizycznej
- Nadawca przesyłając informacje wskazuje adres sprzętowy odbiorcy. Każda stacja dostaje wszystkie ramki, ale jej interfejs sieciowy porównuje adres stacji z adresem zawartym w ramce i może odrzucać ramki przeznaczone dla innych stacji

Adresy sprzętowe - cd

- Format adresów zależy od rodzaju sieci
- Przypisywanie adresów:
  - adresy statyczne
  - adresy dynamiczne
  - adresy konfigurowalne
- Każdy interfejs sieciowy musi rozpoznawać swój własny adres, a często także adres rozgłoszeniowy i adres rozgłaszania grupowego

Ramka sieci fizycznej

- W sieciach pakietowych dane przesyłane są w małych porcjach – *ramkach* (ang. *frames*)
- Karta sieciowa musi być w stanie rozpoznać początek i koniec ramki

  Na początku ramki przesyłana jest specjalna sekwencja bitów - *synchronizacja*

ramka IEEE 802.3

Ramki sieci fizycznej - cd

- Ramka przeważnie zawiera w nagłówku zarówno adres fizyczny nadawcy, jak i odbiorcy
- Adresy te pozwalają zidentyfikować nadawcę i odbiorcę ramki, ale nie rodzaj informacji w ramce.
- Rodzaje ramek:
  - ramki samoidentyfikujące się (o jawnym typie)
  - ramki bez identyfikacji (o niejawnym typie)

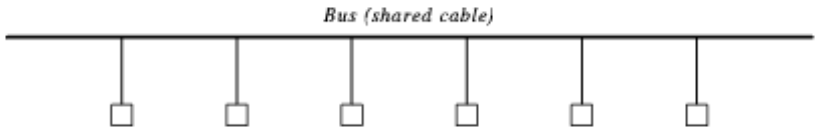
Standardy sieciowe

Standard sieciowy definiuje m.in.:

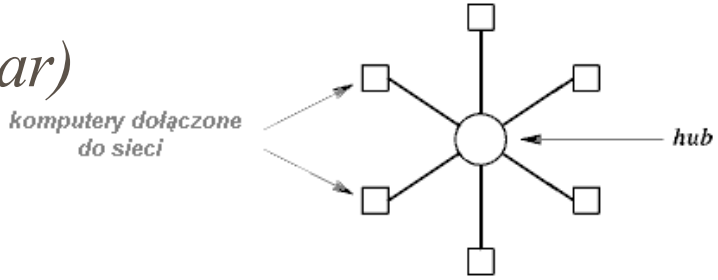
- topologię fizyczną
  (sposób połączenia)
- topologię logiczną
  (sposób komunikacji)
  - format ramek
  - zasadę dostępu do medium transmisyjnego
  - adresy fizyczne (postać, sposób ich nadawania)

Podstawowe topologie (fizyczne) sieci LAN

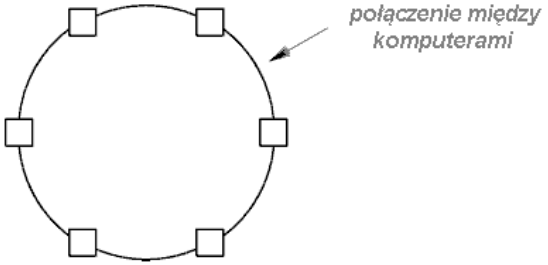
- topologia szyny (magistrali) *(*ang. *bus)*



- topologia gwiazdy *(*ang. *star)*

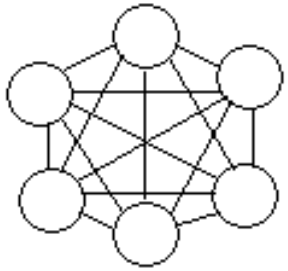


- topologia pierścienia *(*ang. *ring)*

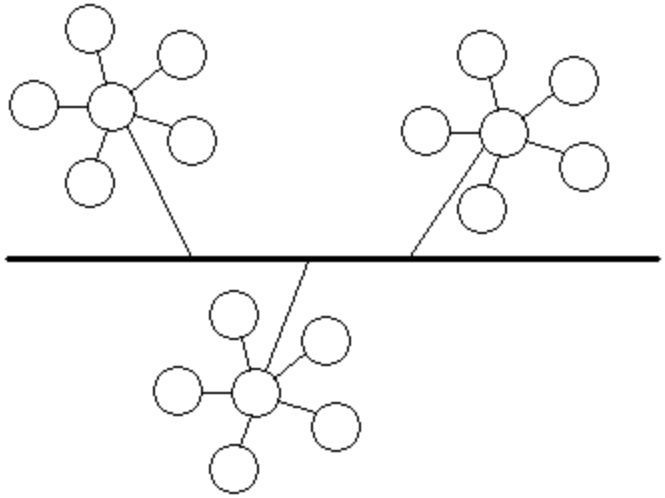


Podstawowe topologie fizyczne - cd

- topologia siatki *(mesh)*



- topologia drzewiasta *(tree)*



Podstawowe topologie logiczne

Mówiąc o topologiach logicznych, wyróżnia się niekiedy:

- topologię rozgłoszeniowa (*broadcast*)
- topologię z przekazywaniem znacznika *(token passing)*

Standard Ethernet

- przykład sieci o topologii szyny
  - zaprojektowany w latach 70-tych jako „Experimental Ethernet”; ok. 3Mbps
  - formalna specyfikacja – standard DIX (Digital – Intel - Xerox), 10Mbps; 1980r.
  - Standard IEEE 802.3 (1985r.), tzw. 10Base-5. Istnieje wiele odmian, np. 802.3a (10Base-2), 802.3i (10Base-T), 802.3 j(10Base-F), 802.3u (100Base-T4,100Base-TX, 100Base-FX), 802.3z (1000Base-F), 802.3ab (1000Base-T), 802.3ae (10000Base-F)

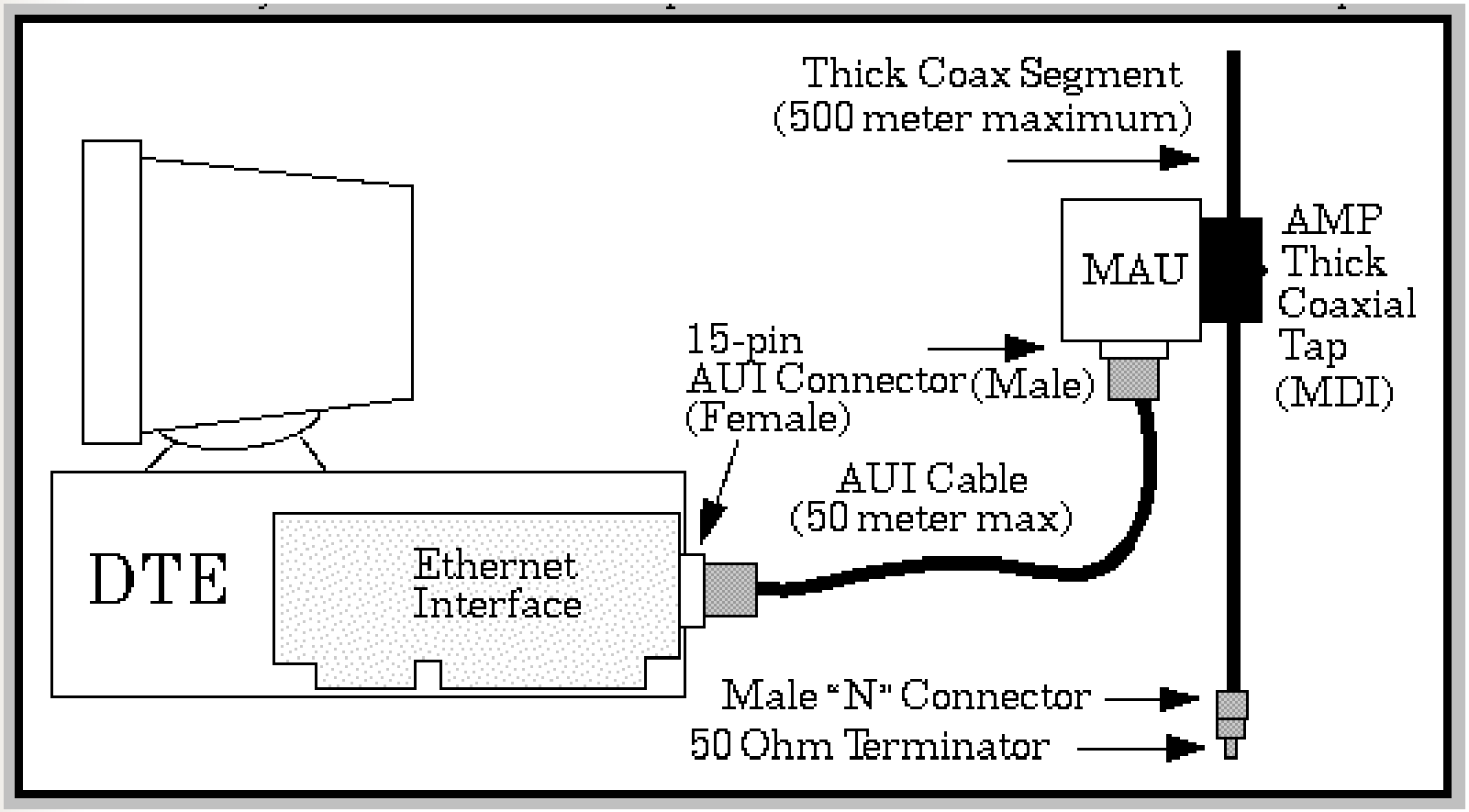
Schemat oznaczania:

- Przepustowość (Mbps) – 10, 100, ...
- Rodzaj transmisji:
  - Base – w paśmie podstawowym
  - Broad – w rozszerzonym
- Rodzaj zastosowanego medium
  - 2 – cienki kabel koncentryczny (thin ethernet)
  - 5 – gruby kabel koncentryczny (thick ethernet)
  - T – skrętka (twisted pair)
  - F – światłowód (fiber optic)
- Dodatkowe oznaczenia
  - np. X – transmisja w skrętce po jednej parze w każdą stronę, L – zwiększona długość segmentu i inne

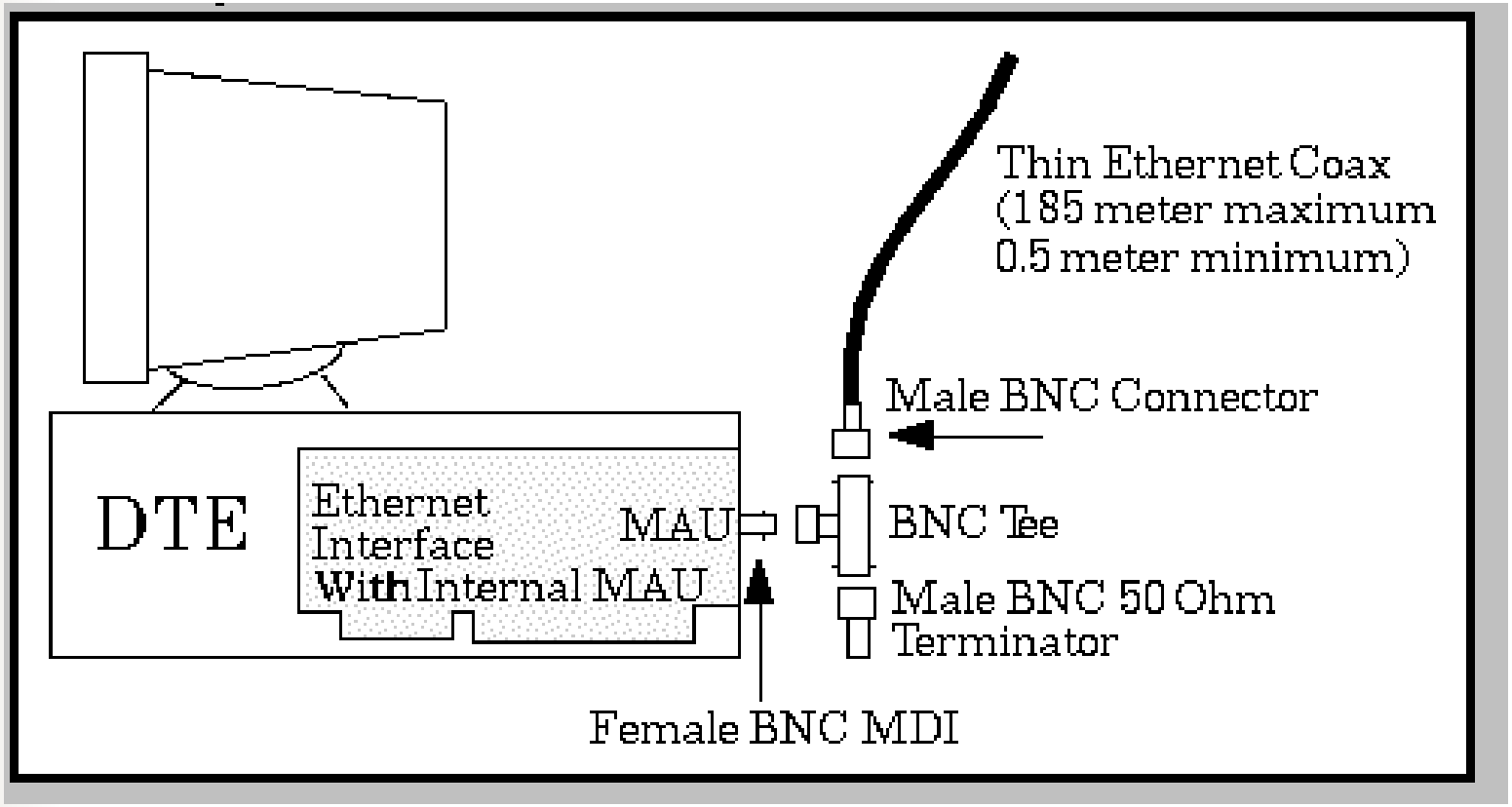
Rodzaje kabla koncentrycznego

- tzw. gruby eternet – 10Base5 - ThickNet (kable 50Ω RG-58 i RG-11); ograniczenie długości do 500m
- tzw. cienki eternet – 10Base2 – ThinNet (kable 50Ω RG-58); ograniczenie długości do około 200m

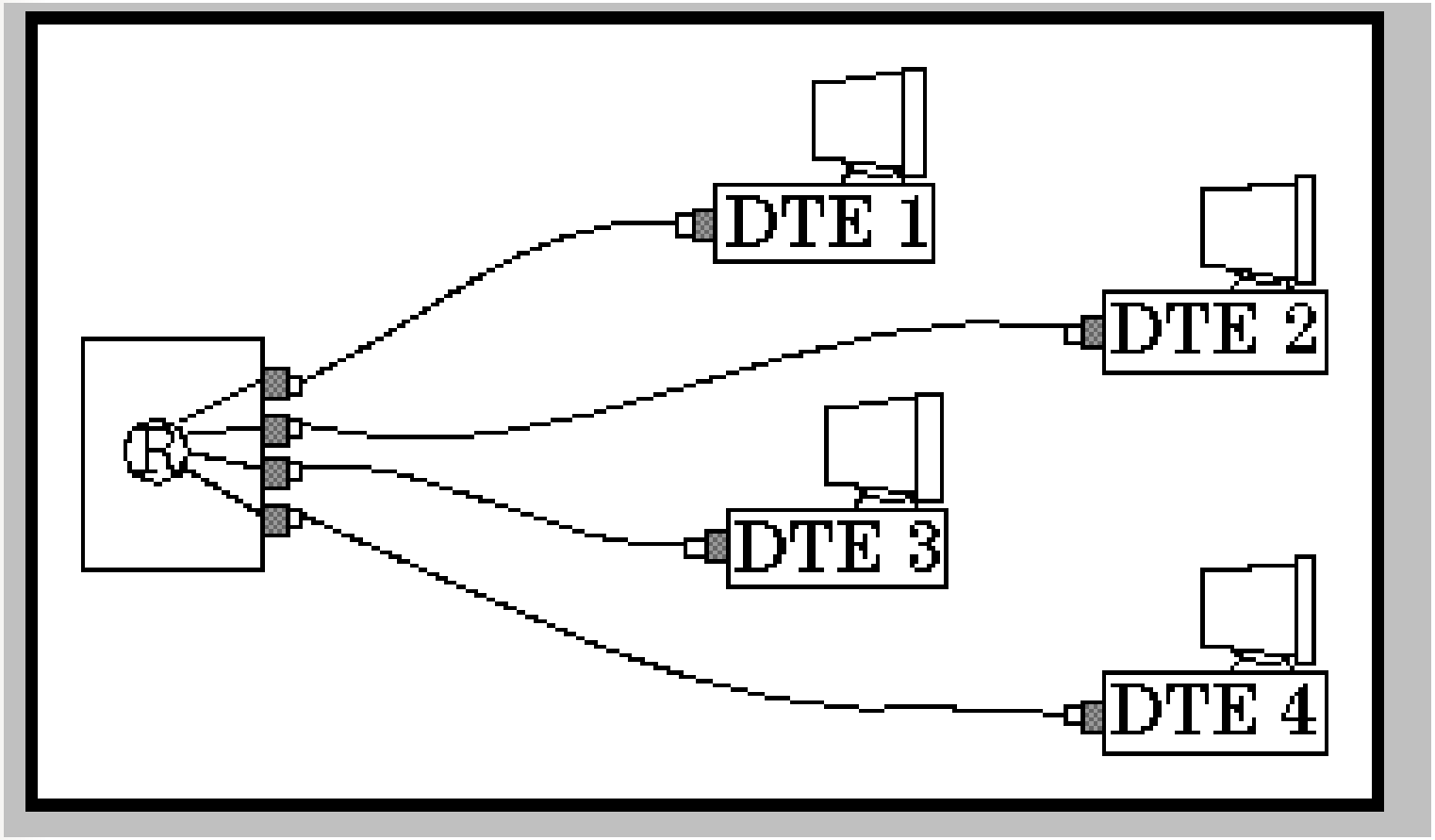
Gruby Ethernet – podłączenie



Cienki Ethernet - podłączenie

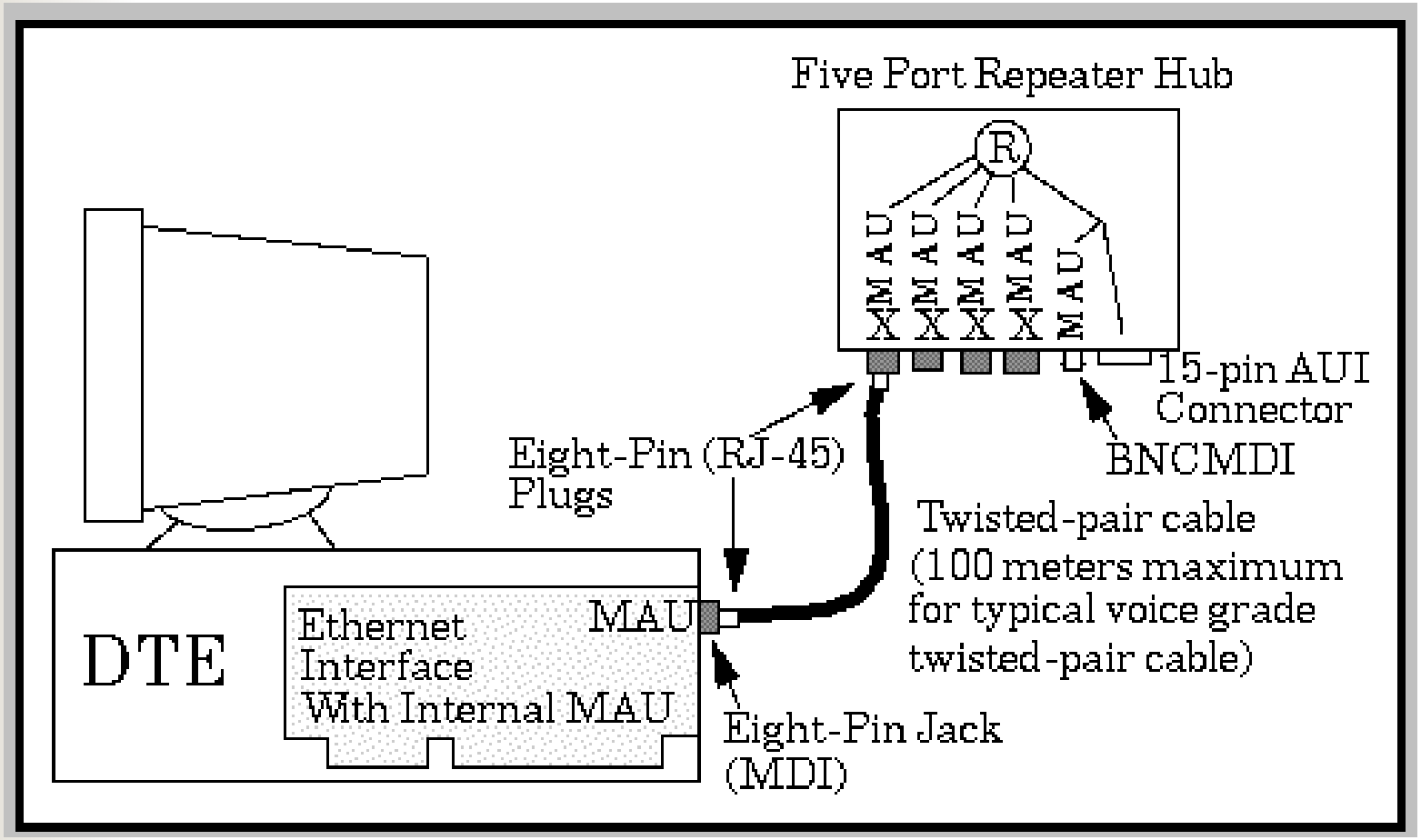


Skrętka telefoniczna - połączenia

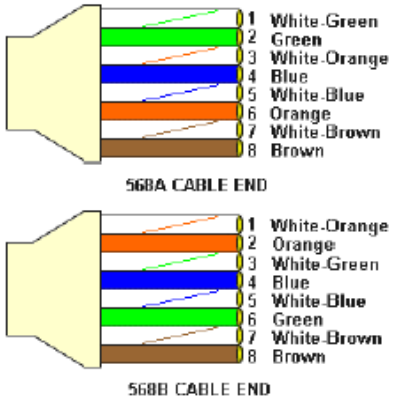


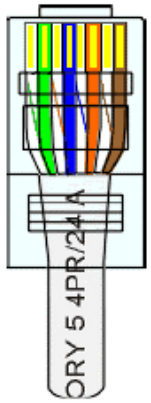
Złącza – cienki Ethernet

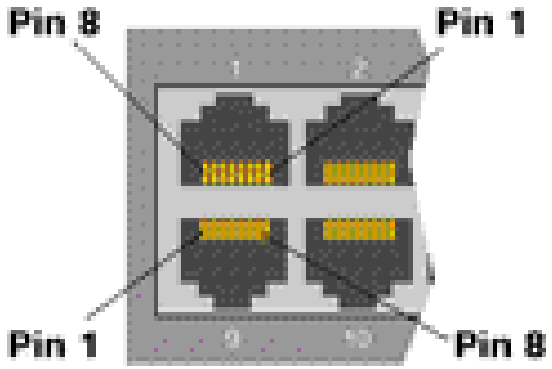
Skrętka – połączenie - cd

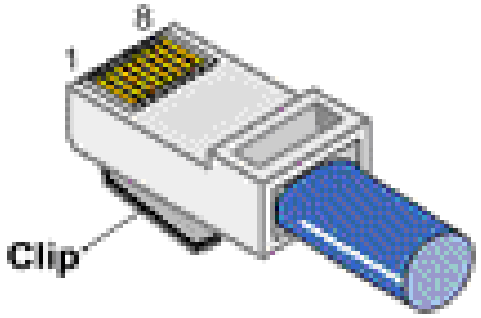


Skrętka telefoniczna - złącza







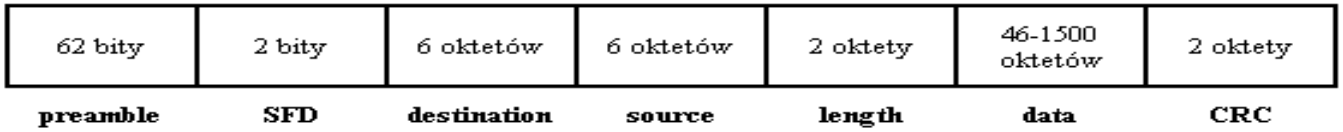


Adresy sprzętowe

- Z każdym interfejsem hosta skojarzony jest unikalny adres sprzętowy (hardware address, physical address, MAC address). Zmiana karty sieciowej komputera powoduje zmianę jego adresu sprzętowego
- Adres w sieci Ethernet jest 48-bitowy

  (np. 00:0C:F1:30:95:0A)
- Typy adresów:
  - adres pojedynczego komputera *(unicast address)*
  - adres rozgłoszeniowy *(broadcast address)* – same jedynki
  - adres rozsyłania grupowego *(multicast address)*

Ramka 802.3

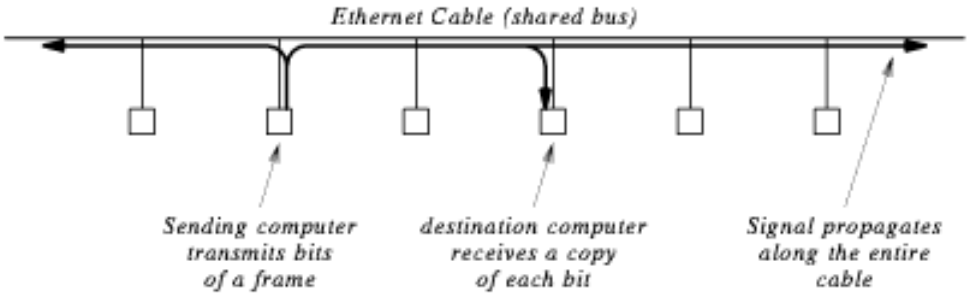


ramka IEEE 802.3

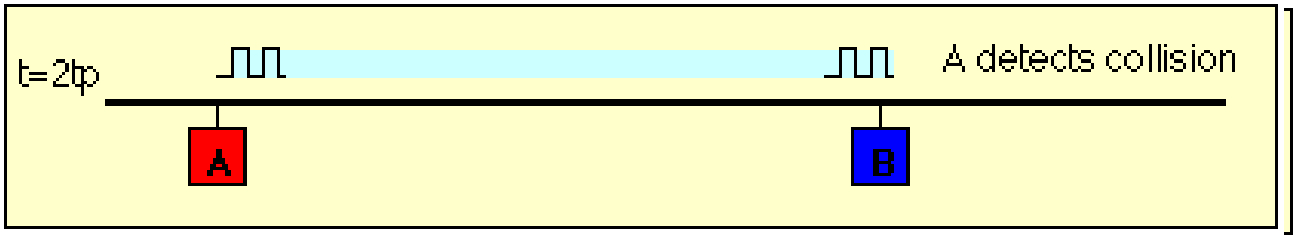
- Poszczególne pola w ramce:
  - preambuła – ciąg bitów złożony z następujących na przemian zer i jedynek
  - SFD (start frame delimiter) – dwie jedynki, początek właściwej zawartości
  - destination – 48-bitowy adres fizyczny odbiorcy
  - source – 48-bitowy adres fizyczny nadawcy
  - length – ilość bajtów w polu danych
  - data (dane) – od 46 do 1500 oktetów; w przypadku mniejszej ilości danych do przesłania pole jest dopełniane do tej wartości (ang. *padding*). Pole *length* zawiera wówczas liczbę istotnych danych
  - CRC – suma kontrolna obliczana dla pól od *destination* do *data* włącznie

Protokół CSMA/CD

- Protokół dostępu do medium transmisyjnego w sieci Ethernet
- CSMA/CD oznacza *Carrier Sense Multiple Access with Collision Detection* – wykrywanie fali nośnej w łączu wielodostępnym z równoczesnym wykrywaniem kolizji
- kolizja – sytuacja gdy kilka stacji transmituje równocześnie

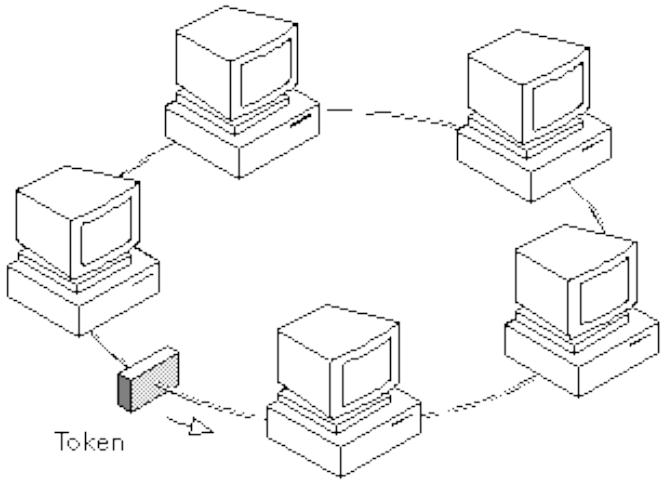


Kolizja w sieci Ethernet



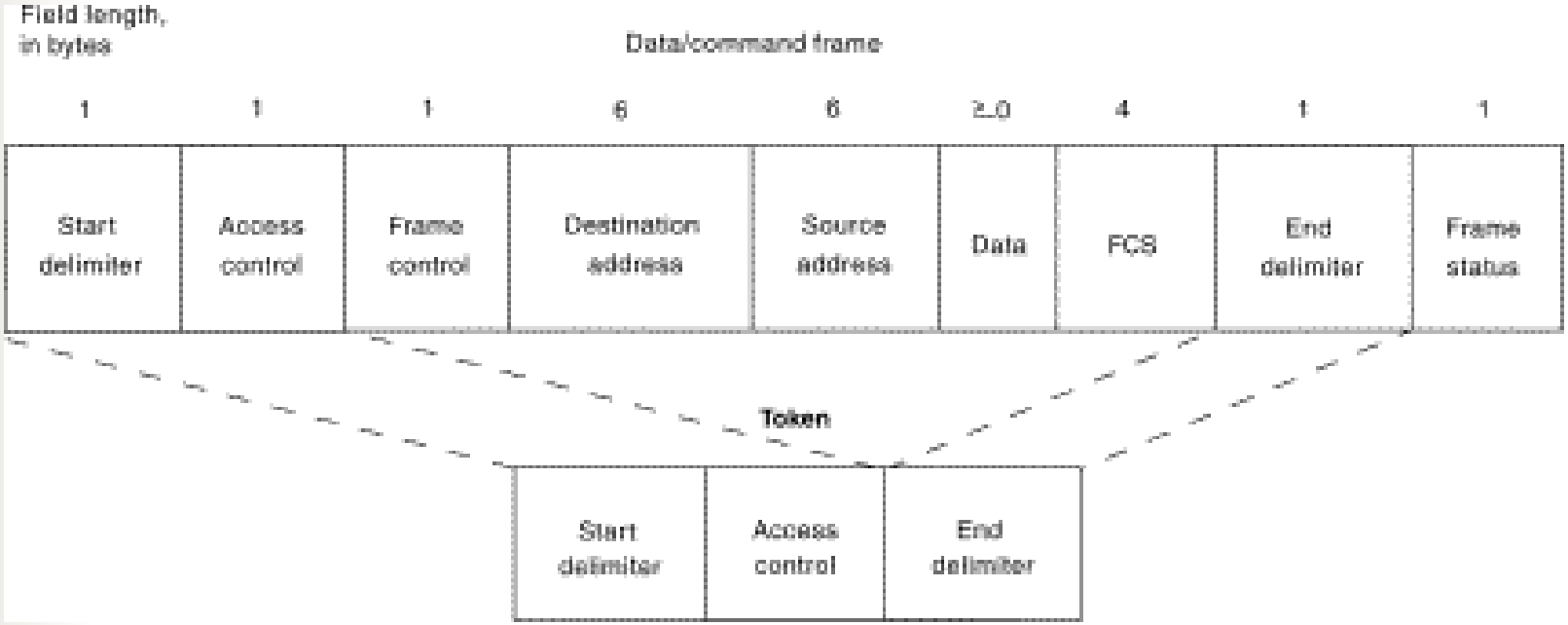
- po wykryciu kolizji A i B przerywają transmisję i wysyłają sygnał powiadamiający o kolizji (tzw. *jam*)
- ponowna próba transmisji następuje po czasie wylosowanym z pewnego ustalonego przedziału
- jeśli kolejna próba zakończy się niepowodzeniem (kolizją), to czas odczekiwania losowany jest z przedziału dwukrotnie większego
- podejmowane jest do 16 takich prób

Standard Token Ring

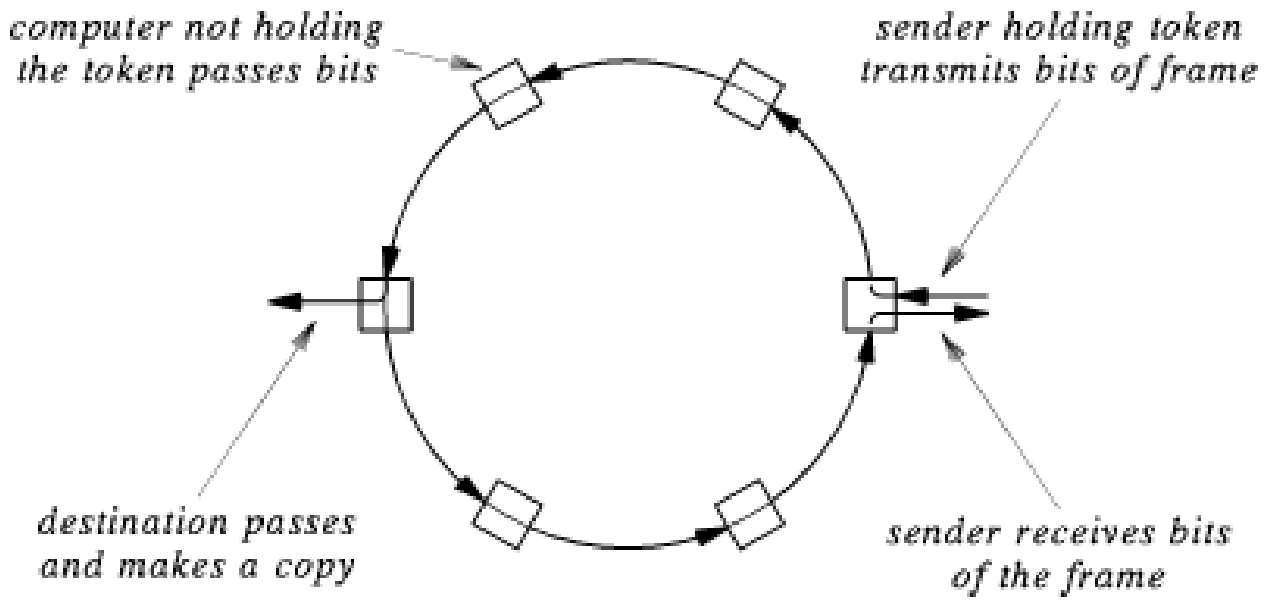


- topologia pierścieniowa
- prawo transmisji ma stacja posiadająca *znacznik* (ang. *token*)
- 4-16 Mbps

Ramka Token Ring



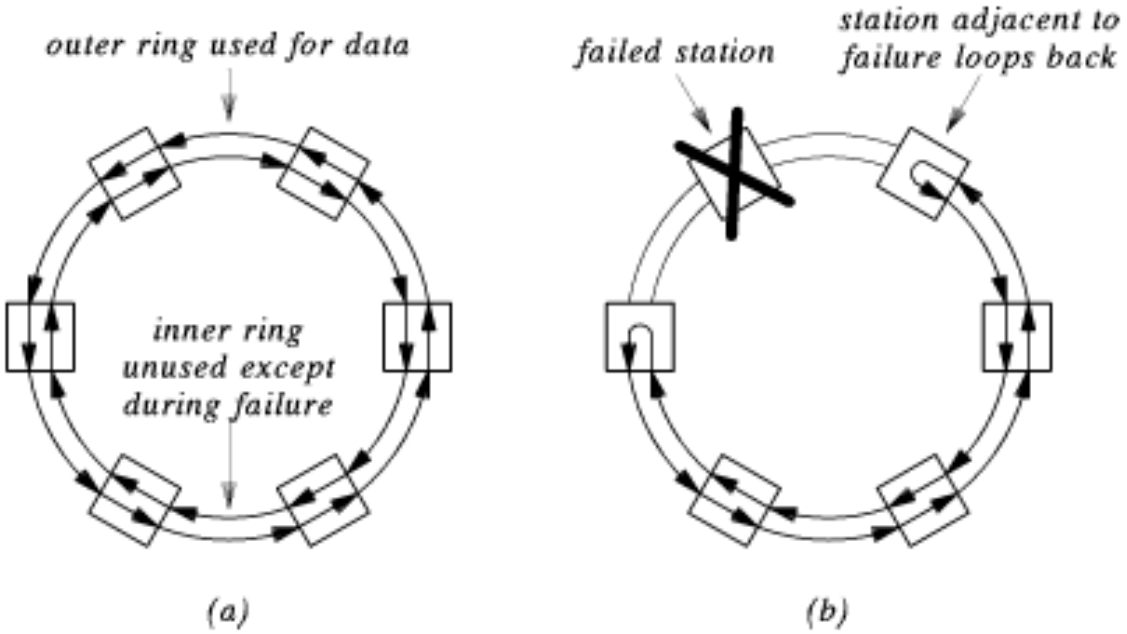
Przekazvwanie znacznika



Standard FDDI

- topologia pierścienia z przekazywaniem znacznika
- łącza światłowodowe
- transmisja do 100Mbps, FDDI-2 – do 200 Mbps
- używane w charakterze szkieletów (*backbone*) sieci WAN
- podwójny pierścień

FDDI - cd


outer ring used for data
inner ring
unused except
during failure
(a)
failed station
station adjacent to
failure loops back
(b)

Samoregeneracja pierścienia

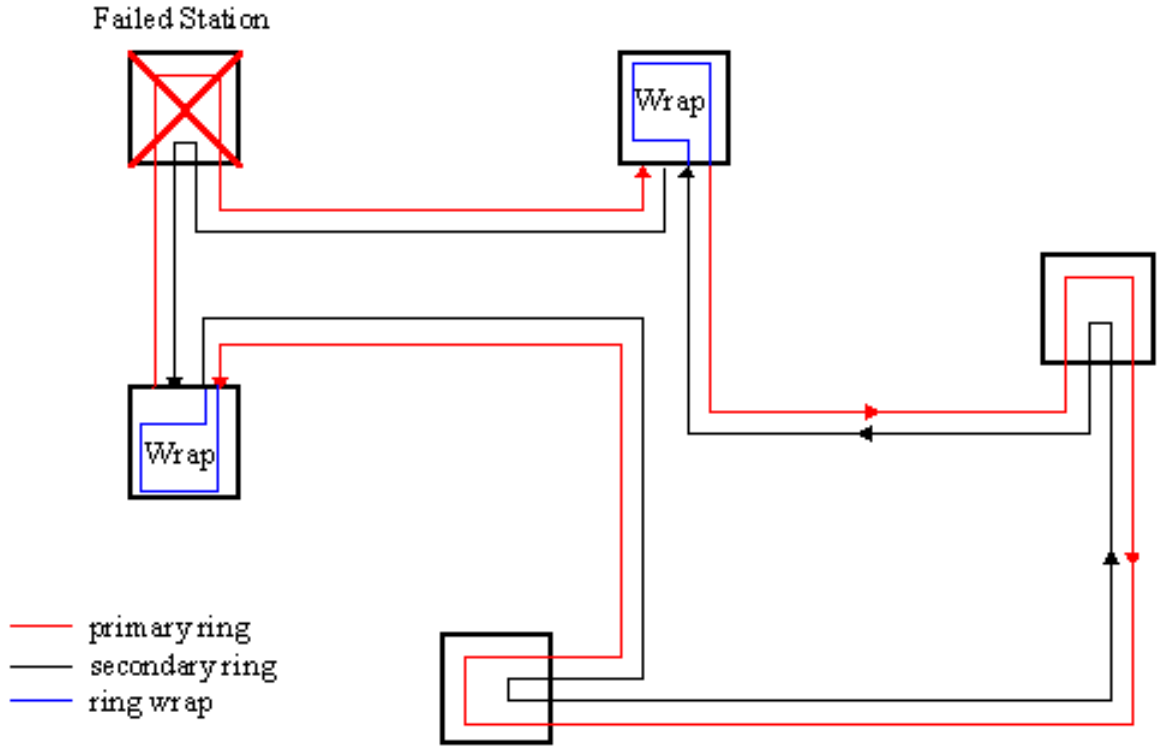
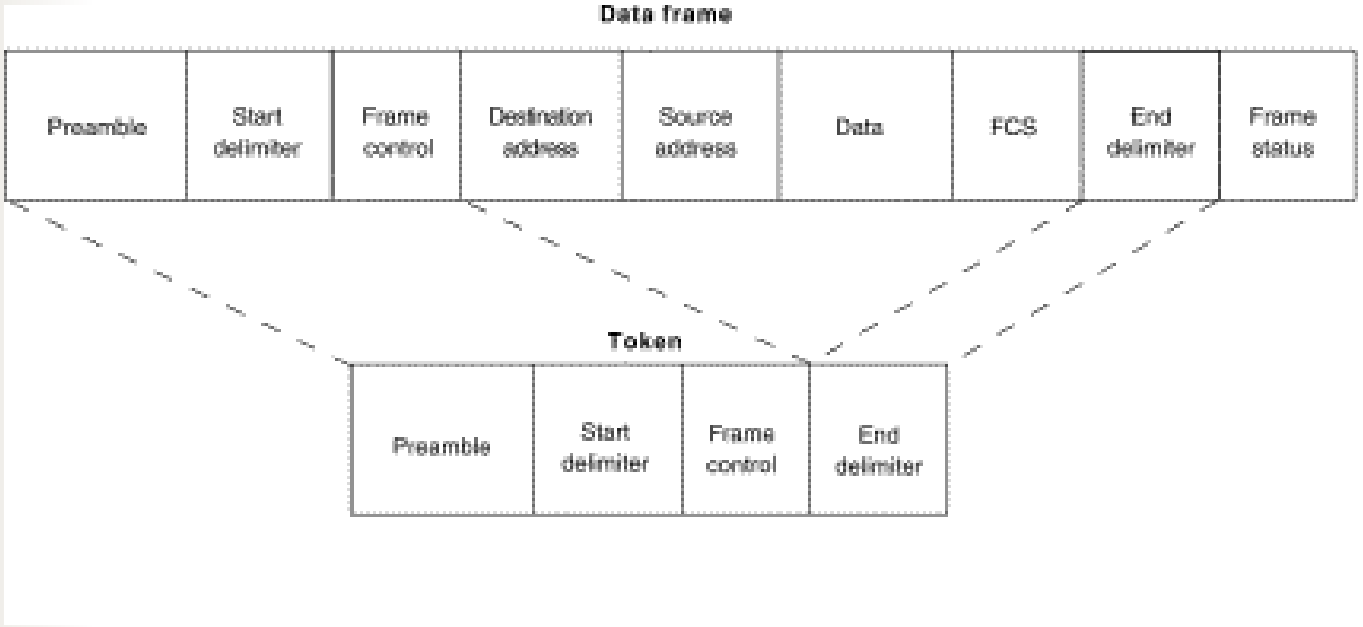


Figure 1: Station failure in FDDI

Ramka FDDI


Data frame
Preamble
Start delimiter
Frame control
Destination address
Source address
Data
FCS
End delimiter
Frame status
Token
Preamble
Start delimiter
Frame control
End delimiter

Zwiększanie rozmiarów sieci

Urządzenia sieciowe

- wzmacniak (repeater)
  - amplifier (wzmacnia sygnały wraz z szumem);
  - signal regenerating repeater (regeneruje sygnał)
- koncentrator (hub, repeater wieloportowy)
  - active hub (regeneruje sygnał)
  - passive hub
- przełącznik (switch) - przek. sygnał do odp. segmentów
- most (bridge) - zwiększa dł. segmentu, separuje ruch
  - mosty uczące się *(learning bridges)*
- router - łączy kilka logicznie oddzielnych sieci

Adresowanie w sieciach

Sieć fizyczna

- W sieciach o wspólnym medium sygnał wysyłany przez jedną stację dociera do wszystkich innych.
- Interfejs sieciowy każdej stacji odbiera sygnał elektryczny i odczytuje przesłaną ramkę
- Wymiana informacji przeważnie nie dotyczy wszystkich stacji naraz.

Adresy sprzętowe

- Adresy sprzętowe (inaczej fizyczne, MAC adresy) identyfikują jednoznacznie interfejs w sieci fizycznej (adres - liczba)
- Nadawca przesyłając informacje wskazuje adres sprzętowy odbiorcy
- Każda stacja dostaje wszystkie ramki, ale jej interfejs sieciowy porównuje własny adres z adresem w ramce i odrzuca ramki adresowane do innych stacji

Adresy sprzętowe – c.d.

- Sprzętowy interfejs sieciowy działa niezależnie od procesora, zatem adres sprzętowy chroni komputer przed reagowaniem na ramki nie skierowane do niego

- Ramka przeważnie zawiera dwa adresy sprzętowe: adres nadawcy i adres odbiorcy. Umieszczenie adresu nadawcy ułatwia odbiorcy przesłanie odpowiedzi.

Adresy sprzętowe – c.d.

- Format adresów jest różny w różnych sieciach
- Sposoby przydziału adresów:
  - statyczne (przydzielane interfejsom przez producenta)
  - konfigurowalne (przydzielane przez użytkownika sprzętu sieciowego)
  - dynamiczny (przydzielane w momencie uruchamiania stacji, np. losowane dopóki nie trafi się na adres nie używany przez inny komputer)
- Adresy w danej sieci nie mogą się powtarzać

Adresy sprzętowe – c.d.

- Wiele programów sieciowych korzysta z metody nazywanej rozgłaszaniem *(broadcast)* – wysyłania danych przeznaczonych dla wszystkich komputerów w sieci
- Schemat adresowania musi umożliwiać podanie specjalnego adresu rozgłaszania *(broadcast address)*

Adresy sprzętowe – c.d.

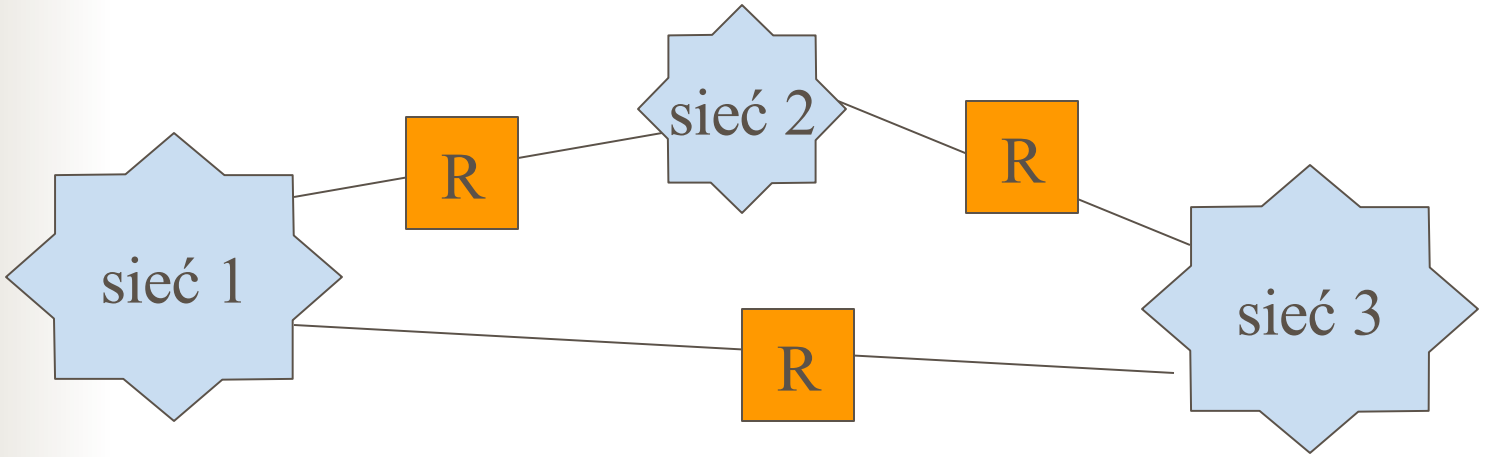
- Wada rozgłaszania – każdy komputer otrzymujący tak zaadresowane ramki musi je przetworzyć
- Rozsyłanie grupowe *(multicasting)*
  - na najniższym poziomie działa jak rozgłaszanie (ramka dociera do wszystkich), jednak interfejs sieciowy jest wcześniej zaprogramowany tak, by rozróżniał ramki rozsyłane grupowo, które powinien akceptować, od tych które należy odrzucić

Adresy sprzętowe – c.d.

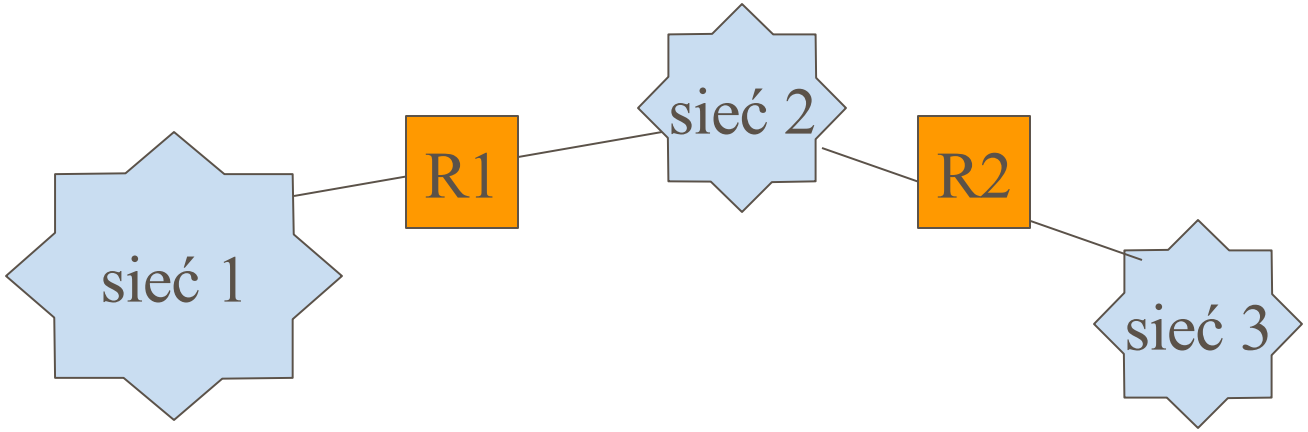
- Każdy interfejs musi zatem rozpoznawać:
  - swój własny adres sprzętowy
  - adres rozgłoszeniowy
  - opcjonalnie – adres rozgłaszania grupowego

Łączenie sieci fizycznych

- Poprzedni schemat adresowania dotyczył pojedynczej sieci fizycznej
- Poszczególne sieci fizyczne łączymy ze sobą używając tzw. routerów (bram IP)



Łączenie sieci – c.d.



- Na tym poziomie nie jest istotne jakiego medium używają sieci i jaki mają rozmiar
- Router R1 musi umieć zdecydować, które komunikaty z sieci 1 mają trafić do sieci 2 lub 3 i wysłać je tam

Łączenie sieci – c.d.

- Router podejmuje decyzję dokąd skierować komunikat (pakiet) na podstawie informacji na temat docelowej sieci (a nie docelowej maszyny)

- Z punktu widzenia użytkownika praca wygląda tak, jakby komputer był dołączony do pojedynczej sieci fizycznej, a nie do intersieci

Komunikacja w intersieci

Obiekty w internecie identyfikowane są przez:

- nazwy (*names*) mówiące czym jest obiekt,
- adresy *(addresses)* mówiące gdzie on jest,
- trasy *(routes)* mówiące jak do niego dotrzeć.

Adresowanie IP

IP – *Internet Protocol*

- Projektanci TCP/IP wybrali system adresów analogiczny do adresów fizycznych
- Każdy komputer w sieci TCP/IP ma przypisany unikatowy adres, będący 32-bitową liczbą całkowitą
- Adres ten jest używany przy wszystkich operacjach wymiany informacji z daną maszyną

Adresy IP – c.d.

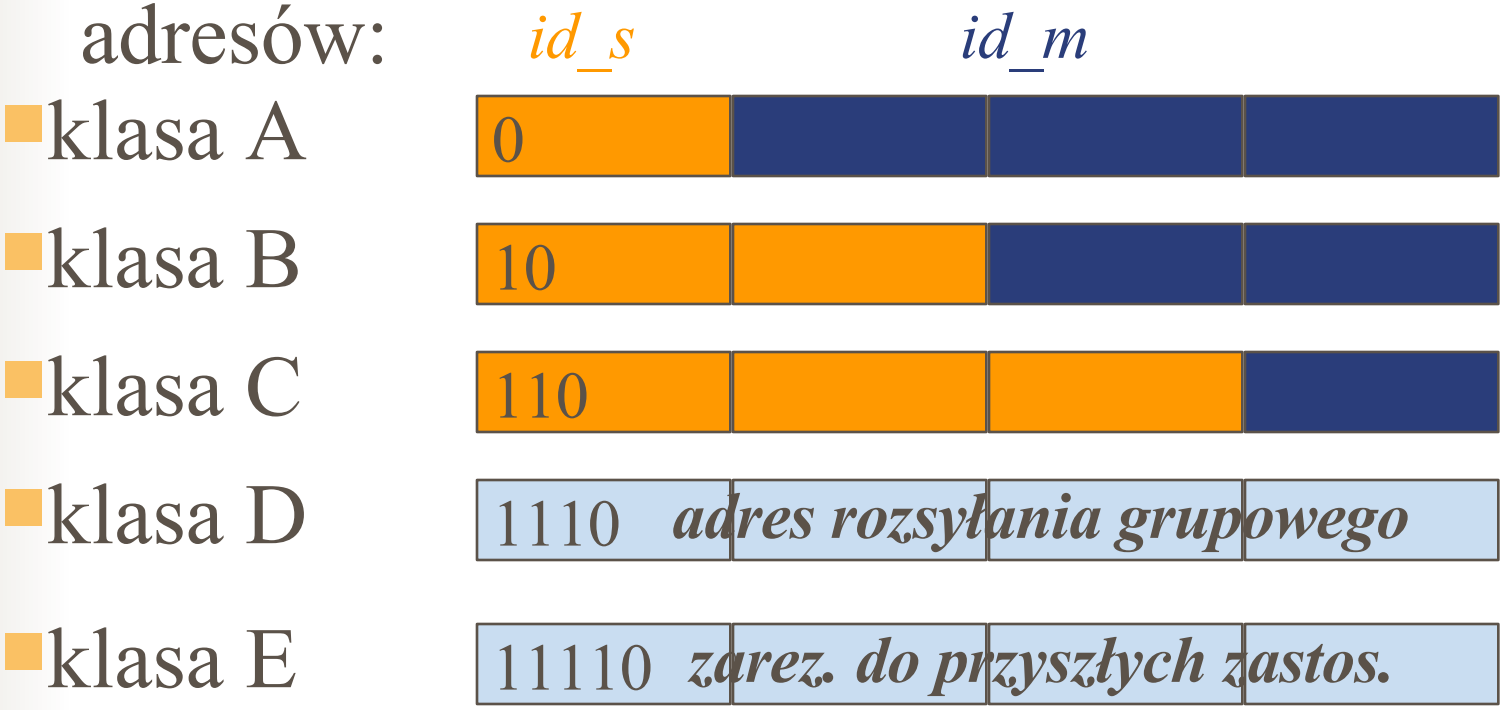
- Adres 32-bitowy:

212 . 191 . 65 . 2

- Każdy adres IP można uważać za parę (*id_s*, *id_m*), gdzie *id_s* – identyfikator sieci, *id_m* - identyfikator maszyny w tej sieci

Klasy adresów IP

- podział (poniekąd nieaktualny) na klasy adresów:



Adresy IP – c.d.

- Adres IP zapisywany jest w postaci czterech liczb całkowitych oddzielonych kropkami. Każda z liczb odpowiada wartości oktetu (bajtu) w adresie

  np:

  `10000000 00001010 00000010 00011110`

  zapisujemy jako

  128.10.2.30

Zakresy adresów

- Klasa A:
  - **1.0.0.0 – 126.0.0.0**
  - 127 sieci po 16.772.214 hostów każda
- Klasa B:
  - **128.1.0.0 – 191.255.0.0**
  - 16.382 sieci po 65.534 hosty każda
- Klasa C:
  - **192.0.1.0 – 223.255.255.0**
  - 2.097.150 sieci po 254 hosty każda
- Klasa D:
  - **224.0.0.0 – 239.255.255.255**
- Klasa E:
  - **240.0.0.0 – 247.255.255.255**

Szczególne przypadki adresów: numery sieci

- Adres, w którym wszystkie bity części przeznaczonej na numer hosta są zerami, interpretuje się jako numer sieci

126.0.0.0

152.12.0.0

213.135.36.0

Szczególne przypadki adresów: adresy rozgłoszeniowe

- Adresy IP mogą być użyte do określenia rozgłoszenia. Jeśli to możliwe, to taki adres jest odwzorowywany na rozgłoszenie sprzętowe.
- W adresie rozgłoszeniowym wszystkie bity części przeznaczonej na numer hosta są ustawione na 1

Szczególne przypadki adresów: adresy rozgłoszeniowe – c.d.

- Rozgłoszenie skierowane *(directed broadcast)*:

  sieć 126.0.0.0 : 126.255.255.255

  sieć 152.12.0.0 : 152.12.255.255

  sieć 213.135.36.0 : 213.135.36.255

- Rozgłoszenie ograniczone *(limited broadcast)*:

  255.255.255.255

Szczególne przypadki adresów: c.d.

- Pole złożone z samych jedynek można interpretować jako „wszystkie” (np. rozgłoszenie – wszystkie komputery w sieci)
- Pole złożone z samych zer można interpretować jako „ten” (np. adres IP w którym numer sieci jest zerem odnosi się do „tej” sieci; przykład: 0.0.0.3)
  - ustawienia takie są przydatne, gdy komputer chce komunikować się za pośrednictwem sieci, a nie zna jeszcze swojego adresu IP

Szczególne przypadki adresów: pętla zwrotna *(local loopback)*

- Adres **127.0.0.1** jest zarezerwowany dla tzw. *pętli zwrotnej (local loopback)* i używany do testowania komunikacji między procesami na komputerze lokalnym

Szczególne przypadki adresów – c.d.

- Maska sieci : część przeznaczona na nr sieci zawiera same jedynki, część przeznaczona na nr hosta – same zera

  A: sieć 126.0.0.0 : 255.0.0.0

  B: sieć 152.12.0.0 : 255.255.0.0

  C: sieć 213.135.36.0: 255.255.255.0

- Maskę zapisuje się również liczbą ozn. liczbę bitów w numerze sieci: **126.0.0.0/8**

Rozszerzenia schematu adresów

- Powyższy schemat rozszerzyć można o:
  - adresowanie w podsieciach {*subnetting*}
  - adresy rozsyłania grupowego *(multicasting)*

Maska sieci

- Maska opisuje, które bity przeznaczone są w adresie IP na numer sieci
- Schemat „klas adresów” został obecnie praktycznie zastąpiony przez schemat adres + maska (*podsieci*)
- Jest to spowodowane faktem, że duże różnice rozmiaru między klasami powodowały marnowanie adresów, a w konsekwencji wyczerpanie się przestrzeni adresowej

Dołączenie do wielu sieci

- Komputery dołączone do kilku sieci równocześnie określane są jako tzw. *multi-homed hosts*
- Multi-homed hosts i routery wymagają kilku adresów IP. Każdy adres odpowiada jednemu z podłączeń danej maszyny do sieci
- Adres IP identyfikuje zatem podłączenie (interfejs sieciowy), a nie komputer jako taki

Dołączenie do wielu sieci - cd

- Adres IP określa sieć i urządzenie w tej sieci
- Przeniesienie komputera do innej sieci powoduje zmianę jego IP
- Algorytmy trasowania korzystają z części sieciowej adresu IP. W przypadku podłączenia komputera do kilku sieci (a więc mającego kilka adresów IP) wybór trasy zależy od użytego adresu.

Protokół ARP

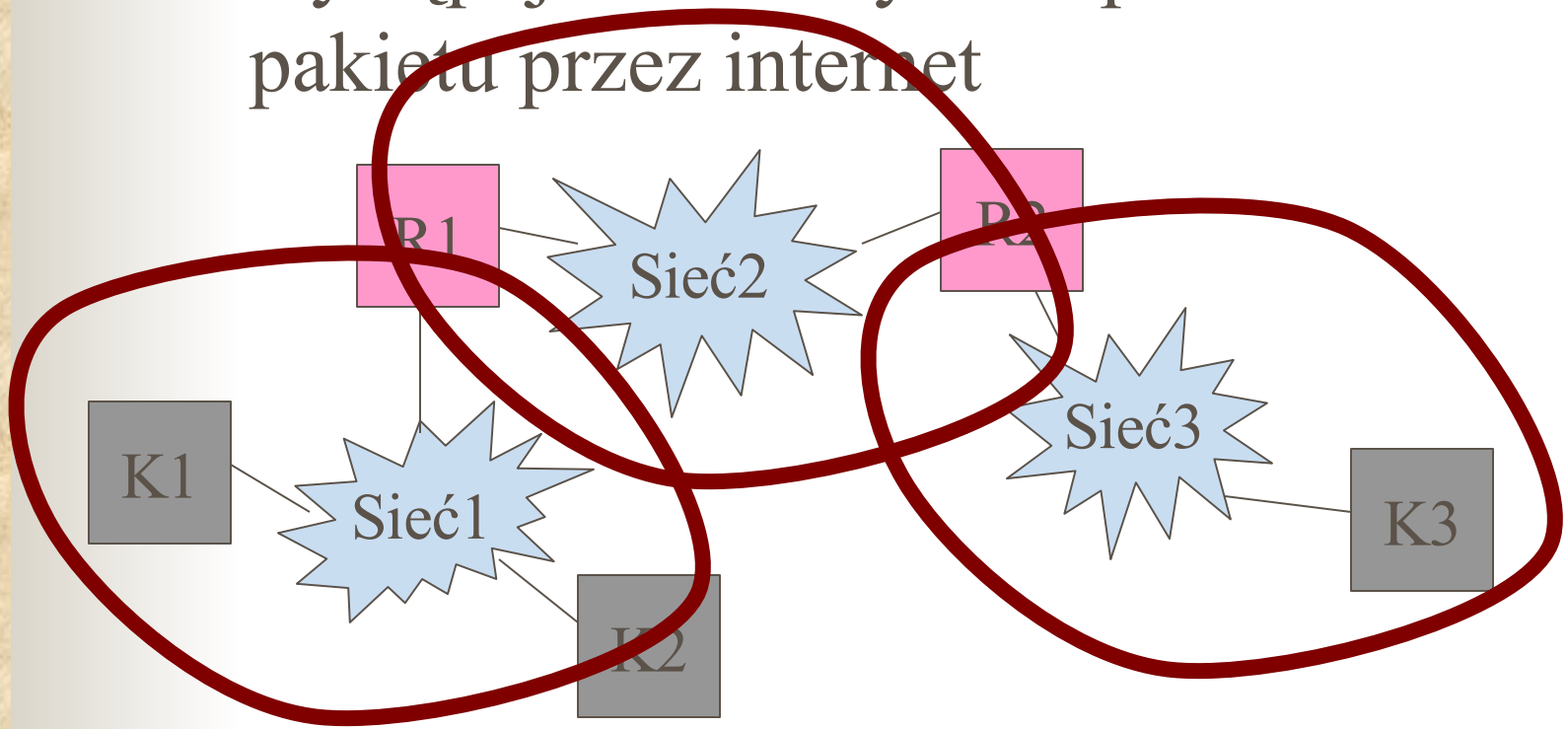
Schemat komunikacji

- W schemacie adresowania TCP/IP każdy węzeł sieci ma przypisany 32-bitowy adres IP. Przy wysyłaniu i odbieraniu informacji w Internecie używa się wyłącznie tych adresów
- Dwa urządzenia w danej sieci fizycznej mogą komunikować się tylko wtedy, gdy znają nawzajem swoje adresy fizyczne

- Węzeł lub router, chcąc dostarczyć pakiet siecią fizyczną, musi zatem przekształcić adres IP na odpowiedni adres fizyczny (tzw. *rozwiązywanie adresów*)

Komunikacja za pomocą sieci fizycznej

- Komunikacja za pomocą sieci fizycznej występuje na każdym etapie dostarczania pakietu przez internet



Sposoby rozwiązywania adresów

- odwzorowanie tablicowe
  (każdy komputer pamięta tablicę par adres fizyczny – adres IP dla całej sieci)
- odwzorowanie obliczeniowe
  (adres sprzętowy można wyliczyć z IP)
- odwzorowanie sieciowe (komputery wymieniają komunikaty w celu odwzorowania adresów)

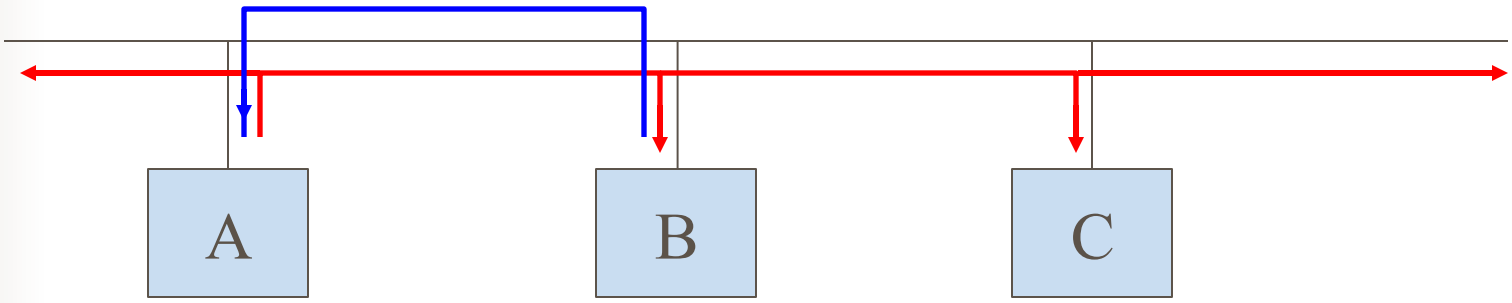
Odwzorowanie przez wymianę komunikatów

W celu odwzorowania adresów komputery mogą wymieniać komunikaty:

- z pewnym centralnym serwerem
  - wady: konieczność aktualizacji bazy, obciążenie serwera
- bezpośrednio między sobą

Protokół ARP

- ARP – *Address Resolution Protocol* – protokół odwzorowywania adresów
- definiuje dwa rodzaje komunikatów: zapytania i odpowiedzi



Schemat działania ARP

- komputer A rozgłasza zapytanie ARP zawierające adres IP komputera B (oraz adres sprzętowy A)
- zapytanie dociera do wszystkich komputerów, B rozpoznaje swoje IP
- B wysyła odpowiedź ze swoim adresem sprzętowym bezpośrednio do A (może to zrobić, gdyż zapytanie zawierało adres sprzętowy A)

Cache ARP

- Dla zredukowania kosztów komunikacji komputery przechowują w pamięci podręcznej (*cache*) ostatnio uzyskane powiązania adresów IP z adresami fizycznymi
- Zawartość cache'a sprawdzana jest przed ewentualnym wysłaniem kolejnego zapytania
- Opłacalne – komunikacja wymaga zazwyczaj przesłania więcej niż jednego pakietu

Cache ARP – modyfikacje

- Możliwe modyfikacje schematu:
  - zapamiętywanie przez B pary (adres_sprzętowy, adres_IP) komputera A jeżeli A wysyła coś do B, to prawdopodobnie wkrótce B wyśle coś do A
  - zapamiętywanie przez wszystkie komputery w sieci pary (adres_sprzętowy, adres_IP) dla komputera A rozgłaszającego zapytanie
  - komputer włączający się do sieci rozgłasza swoją parę (adres_sprzętowy, adres_IP)

Implementacja ARP

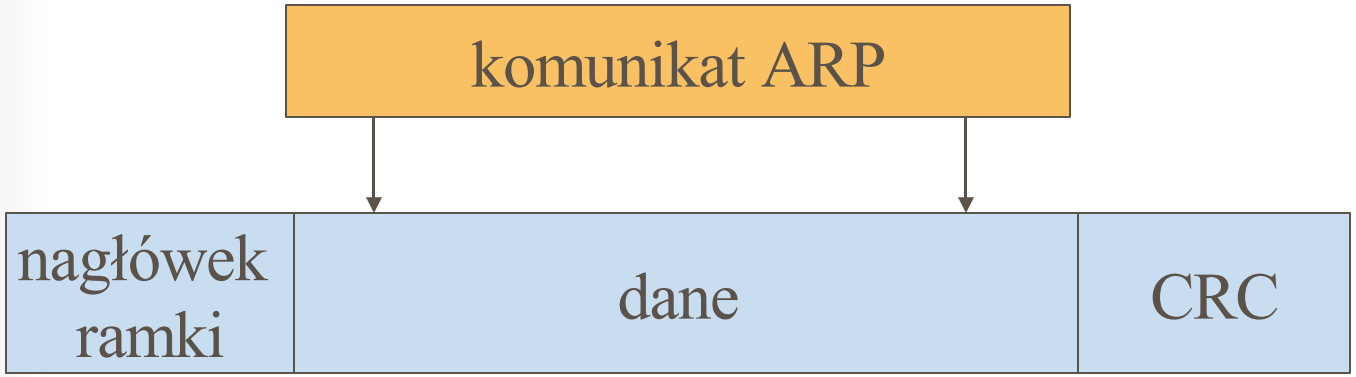
- Części funkcjonalne ARP:
  - odpowiadająca za wysyłanie komunikatów
  - odpowiadająca za obsługę komunikatów przychodzących

ARP a stos protokołów

- ARP to protokół niskopoziomowy, „zasłaniający” podstawowe fizyczne adresowanie w sieci i umożliwiający korzystanie z adresowania IP
- Należy myśleć o ARP jako o części systemu sieci fizycznej, a nie jako o części zestawu protokołów intersieci

Kapsułkowanie ARP

- Komunikaty ARP przenoszone są w ramkach sieci fizycznej (w ich części przeznaczonej na dane)



Format komunikatów ARP

rodzaj sprzętu		rodzaj protokołu
dł. adr.sprz.	dł. adr.prot.	operacja
adres sprzętowy nadawcy		
adres sprzęt. nadawcy -cd		adres IP nadawcy
adres IP nadawcy - cd		adres sprzęt. odbiorcy
adres sprzętowy odbiorcy – cd		
adres IP odbiorcy		

Format komunikatów ARP - cd

- rodzaj sprzętu (adresu sprzętowego) – dla Ethernetu 1
- rodzaj protokołu = rodzaj adresu protokołowego, dla IP 0800_{16}
- operacja: czy jest to prośba ARP (1), odpowiedź ARP (2), prośba RARP (3) czy odpowiedź RARP (4)
- pola długości adresów umożliwiają użycie protokołu w dowolnych sieciach
- poszczególne adresy umieszcza się, jeśli są znane

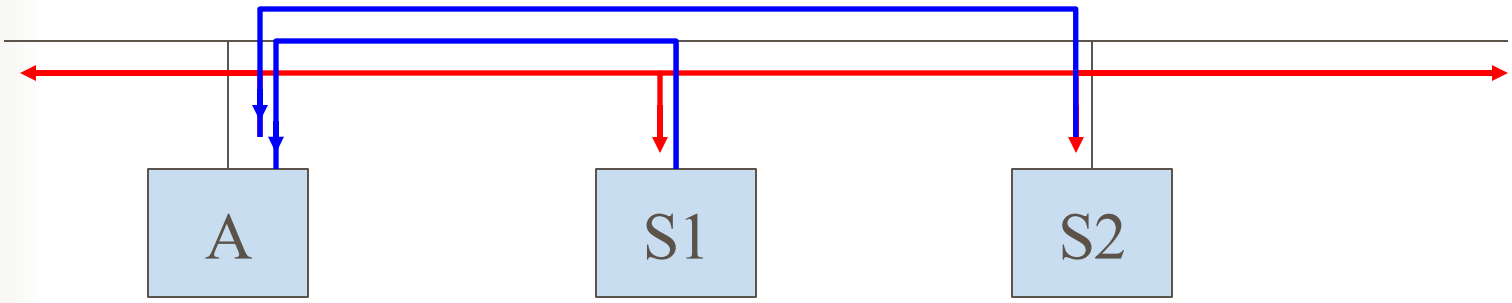
RARP - Reverse ARP

Protokół RARP

- Na bazie ARP powstał protokół RARP
- RARP służy (a raczej służył) do określania adresu IP w momencie rozruchu systemu, jeżeli dany system nie posiadał takiej informacji i musiał w celu jej uzyskania skontaktować się z odpowiednim serwerem
- przodek BOOTP i DHCP

Schemat działania RARP

- A rozgłasza zapytanie RARP, wskazując siebie jako nadawcę
  - Maszyny uprawnione do świadczenia usług RARP odsyłają odpowiedź bezpośrednio do A



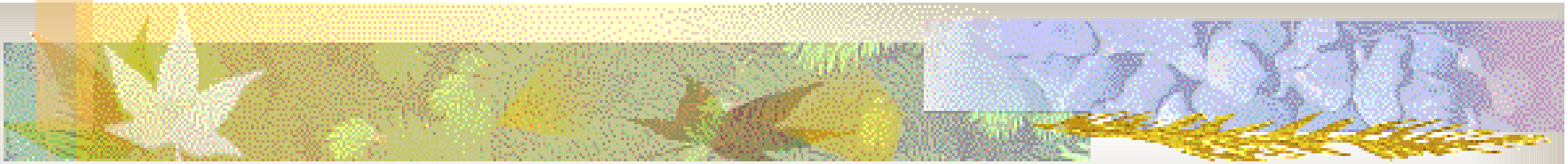
Serwery RARP

- W sieci może być kilka serwerów RARP
  - zwiększa dostępność usługi
  - zwiększa ruch w sieci
- Możliwy schemat: na pierwsze zapytanie klienta odpowiada tylko serwer podstawowy, na kolejne – serwer podstawowy i rezerwowe
- Inny schemat: serwery rezerwowe wysyłają odpowiedzi z opóźnieniem, aby zmniejszyć prawdopodobieństwo kolizji

Właściwości RARP

- Format komunikatów RARP jest taki jak ARP
- Kapsułkowanie analogiczne jak w przypadku ARP

Warstwa sieciowa



Protokół IP
(Internet Protocol)

rysunki na niektórych slajdach w tej części prezentacji pochodzą ze strony
http://www.man.rzeszow.pl/docs/ip/index.html

Usługi w sieciach TCP/IP

- Sieć TCP/IP udostępnia zasadniczo trzy zbiory usług:

- Najbardziej podstawowa usługa intersieci to system przenoszenia pakietów

Usługa przenoszenia pakietów

Usługa ta zdefiniowana jest jako:

- bezpołączeniowa *(connectionless)*

  (każdy pakiet jest obsługiwany niezależnie)
- nie dająca gwarancji *(unreliable)*

  (brak mechanizmów kontrolujących czy pakiet dotarł do adresata)
- wykorzystująca dostępne możliwości *(best-effort)*

  (brak gwarancji dostarczenia wynika z czynników zewnętrznych)

Protokół IP

- Powyższy mechanizm (zawodne bezpołączeniowe dostarczanie pakietów) jest definiowany w protokole intersieci (IP – *Internet Protocol*)

Protokół IP – c.d.

- Protokół IP definiuje:
  - podstawową jednostkę przesyłania danych używaną w sieciach TCP/IP
  - operację trasowania (routingu), wykonywaną przez oprogramowanie IP, polegającą na wyborze trasy przesyłania danych
  - zbiór reguł służących do realizacji bezpołączeniowego dostarczania (sposób przetwarzania pakietów przez hosty i routery, komunikaty o błędach, warunki likwidowania pakietów)

Jednostka przesyłania danych

- Podstawową jednostką przesyłania danych jest datagram IP.
- Datagram składa się z nagłówka i części z danymi, podobnie jak ramka sieci fizycznej

- Datagramy są przetwarzane przez programy (ramki – przez sprzęt), zatem ich format nie jest uwarunkowany sprzętowo

Format datagramu IP

<table>
<tr><td>wersja | dł. nagłówka</td><td colspan="2">typ obsługi</td><td colspan="2">długość całkowita</td></tr>
<tr><td colspan="3">identyfikacja</td><td>znaczniki</td><td>przesunięcie fragmentu</td></tr>
<tr><td>czas życia</td><td colspan="2">protokół</td><td colspan="2">suma kontrolna nagłówka</td></tr>
<tr><td colspan="5">adres IP nadawcy</td></tr>
<tr><td colspan="5">adres IP odbiorcy</td></tr>
<tr><td colspan="4">opcje IP (jeśli potrzebne)</td><td>uzupełnienie</td></tr>
<tr><td colspan="5">dane</td></tr>
</table>

Pola datagramu IP

- wersja – 4 bity – wersja protokołu IP użyta do utworzenia datagramu
- długość nagłówka – w 32-bitowych słowach
  - pola *opcje* i *wypełnienie* często nie są używane (datagram bez opcji) ; pole *długość nagłówka* zawiera wówczas liczbę 5
- długość całkowita - mierzona w oktetach; obejmuje nagłówek i dane
- typ obsługi – pole 8-bitowe, opisujące w jaki sposób należy obsłużyć datagram

Pole „typ obsługi”

- Pierwszeństwo – 3 bity; określa stopień ważności (0 – normalny, 7-sterowanie siecią)
- O – prośba o krótki czas oczekiwania
- S – prośba o przesyłanie szybkimi łączami
- P – prośba o dużą gwarancję przesłania

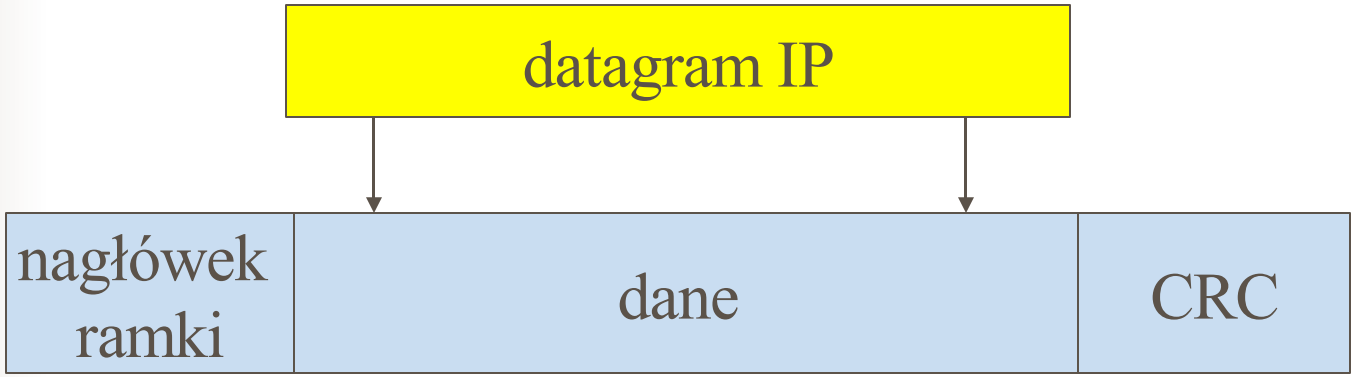
ciąg dalszy pól nastąpi...

Rozmiar datagramów IP

- Ramki sieci fizycznej są obsługiwane przez sprzęt, datagramy przez oprogramowanie. Teoretycznie mogą więc mieć dowolna długość wybraną przez projektanta
- W obecnym formacie datagramu jego maksymalna długość to 65 535 oktetów (wynika to z rozmiaru pola długości całkowitej – 16 bitów)

Przesyłanie datagramów w sieci fizycznej

Datagramy przesyłane są w ramkach sieci fizycznej w części przeznaczonej na dane *(kapsułkowanie)*



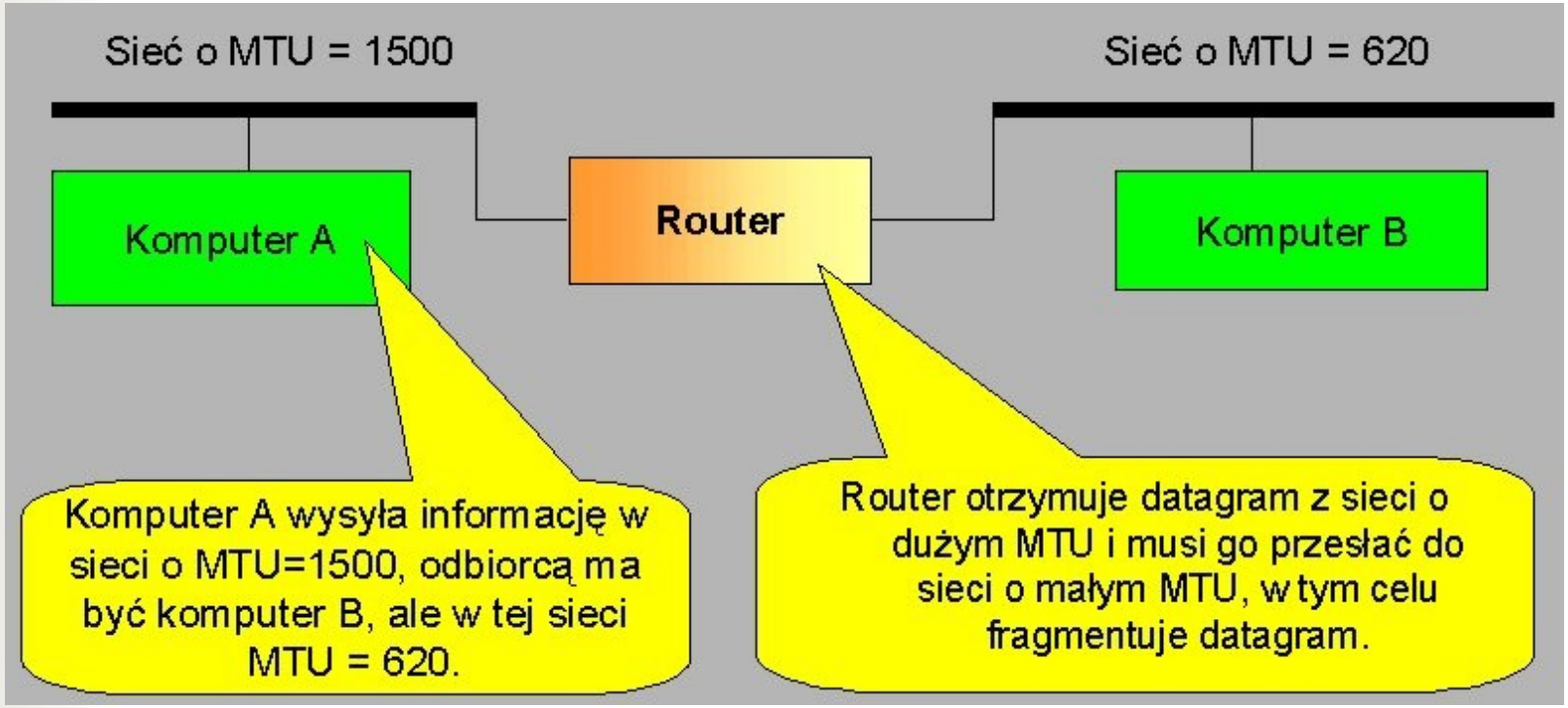
Fragmentacja datagramów

- W idealnej sytuacji każdy datagram mieści się w jednej ramce sieci fizycznej
- Nie zawsze jest to możliwe:
  - Datagram przemieszcza się przez różne sieci fizyczne
  - Każda sieć ma ustaloną górną granicę rozmiaru ramki – tzw. MTU *(maximum transfer unit)* – np. 1500 oktetów w Ethernecie, 4470 oktetów w FDDI

Fragmentacja datagramów - c.d.

- Ograniczenie rozmiary datagramów tak, by pasowały do każdego MTU, byłoby nieefektywne
- Oprogramowanie TCP/IP nadawcy dobiera optymalny rozmiar datagramu
- Jeżeli datagram nie mieści się w ramce sieci fizycznej przez którą ma przejść, to jest dzielony na mniejsze części – fragmenty; proces ten nazywa się fragmentacją

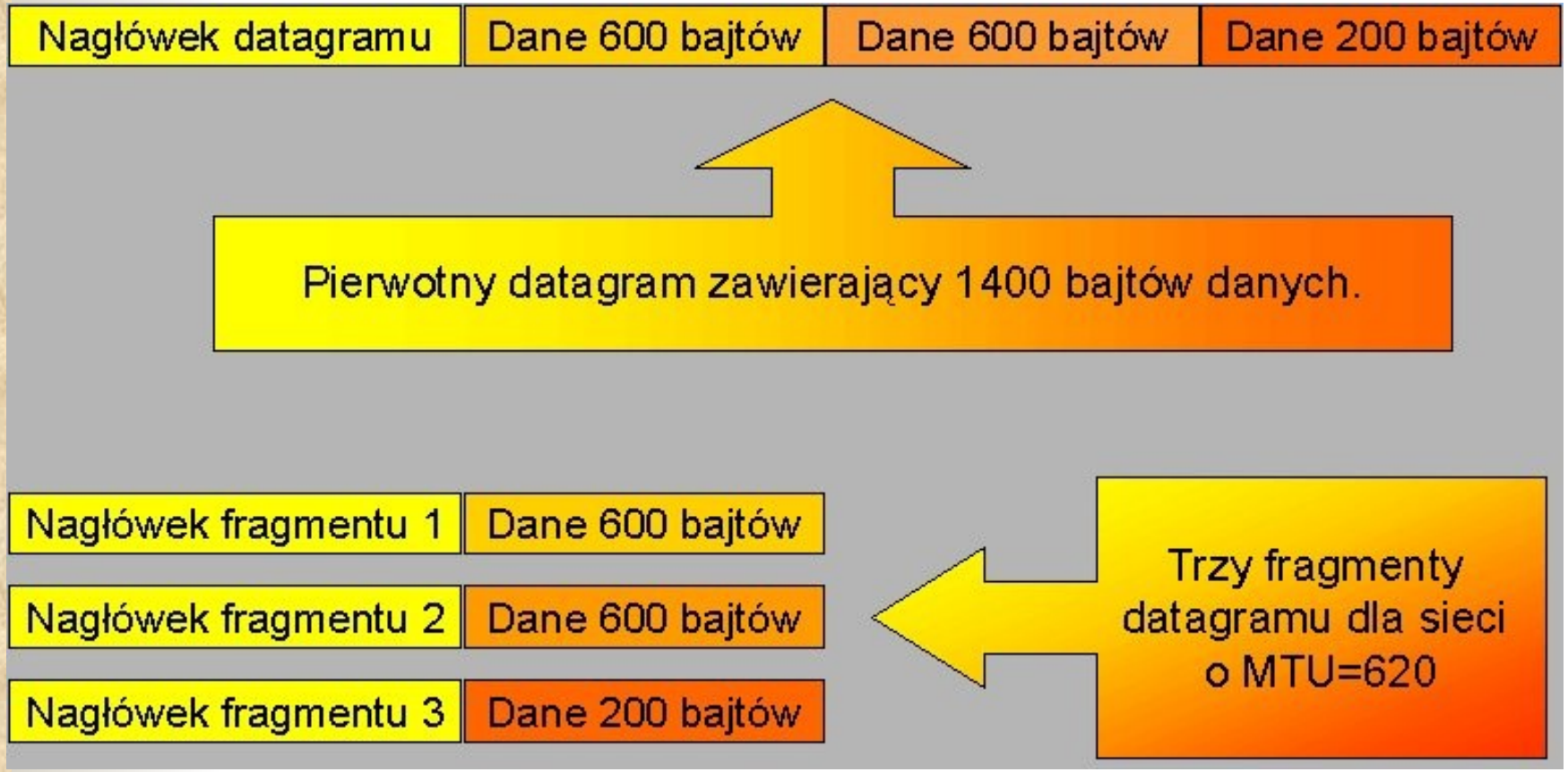
Fragmentacja datagramu – c.d.



Fragmentacja datagramu – c.d.

- Rozmiar fragmentów dobierany jest tak, aby każdy fragment mógł być przeniesiony siecią w pojedynczej ramce
- Rozmiar fragmentów musi być wielokrotnością ośmiu *(wyjaśni się później)*
- Każdy z fragmentów ma format pierwotnego datagramu:
  - zawiera nagłówek, w którym jest powielona większość pól poprzedniego nagłówka
  - zawiera dane – część danych oryginalnego datagramu

Fragmentacja datagramu – c.d.



Fragmentacja datagramu – c.d.

- Poszczególne fragmenty datagramu składane są w całość dopiero u ostatecznego odbiorcy
  - składanie przez routery pośredniczące prowadziłoby do nieefektywności
- Jeżeli pewne fragmenty zostaną zgubione, to datagram nie może zostać scalony
  - po przyjściu początkowych fragmentów odbiorca uruchamia zegar, jeśli wszystkie fragmenty nie przyjdą w wymaganym czasie, to likwiduje to co otrzymał dotychczas

Pola datagramu kontrolujące fragmentację

- Złożenie fragmentów w całość jest możliwe dzięki następującym polom nagłówka:
  - identyfikacja
  - przesunięcie fragmentu
  - znaczniki

Kontrola fragmentacji – c.d.

- identyfikacja – pole o unikalnej wartości; kopiowane do fragmentów
- przesunięcie fragmentu – przesunięcie początku danych datagramu względem początku danych datagramu wyjściowego, mierzone w ósemkach oktetów; ustawiane przy fragmentowaniu
- znaczniki – trzybitowe pole, w tym dwa bity związane z fragmentacją:
  - bit „nie fragmentuj”
  - bit „więcej fragmentów” (ustawiany przy fragmentacji)

Czas życia datagramu

- Pole *czas życia* (TTL – *time to live*) określa, jak długo datagram może pozostawać w sieci
- W przypadku TTL=0 router likwiduje datagram i wysyła komunikat do nadawcy
- Zabezpieczenie przed nieskończonym krążeniem datagramu po sieci

Czas życia datagramu – c.d.

- Urządzenie wprowadzające datagram do sieci nadaje polu „czas życia” pewną wartość
- Routery i węzły przetwarzające datagram zmniejszają wartość tego pola
  - Standardowo – zmniejszenie o 1
  - Obsługa przeciążeń routerów: router rejestruje czas życia datagramu i zmiejsza pole TTL o liczbę sekund, jaką datagram oczekiwał na obsługę
- Jeśli pole „czas życia” osiągnie 0, to router likwiduje datagram

Opcje datagramów

- Pole „opcje IP” występuje tylko w niektórych datagramach
- Obsługa opcji jest integralną częścią IP
- Długość pola – zmienna w zależności od rodzaju opcji
- W każdym przypadku pole zawiera jeden oktet kodu opcji; po nim może pojawić się oktet długości i oktety danych

Opcje datagramów – c.d.

- Oktet kodu opcji jest podzielony na trzy pola:

  - Znacznik *kopiuj* określa jak dana opcja ma być traktowana przy fragmentacji
  - *Klasa opcji* i *numer opcji* w tej klasie określają rodzaj opcji
    - Np. klasa 0 – kontrola datagramów lub sieci
    - Klasa 2 – poprawianie błędów i pomiary

Przykład opcji:
opcja zapisywania trasy (RR)

record route

Kod (7)	długość	wskaźnik
Pierwszy adres IP		
Drugi adres IP		
.....		

- Nadawca tworzy pustą listę adresów
- Każdy router obsługujący datagram umieszcza swój adres IP na liście
  - Pole *wskaźnik* wskazuje pierwsze wolne miejsce w liście opcji

Przykład opcji:
opcja trasowania wg nadawcy

Source route

Kod (17)	długość	wskaźnik
Pierwszy adres IP		
Drugi adres IP		
.....		

- Trasowanie rygorystyczne

  Kolejne adresy wyznaczają dokładną trasę

- Trasowanie swobodne

  Pomiędzy kolejnymi adresami z listy moga występować również inne routery

Przetwarzanie opcji przy fragmentacji

- przy fragmentacji opcje przetwarzane są zgodnie z wartością bitu *kopiuj* w polu *kod*
- Niektóre opcje kopiowane są do wszystkich fragmentów, niektóre umieszczane tylko w jednym (np. RR)

Trasowanie IP
(routing IP)

Protokół IP - przypomnienie

- Protokół IP definiuje:
  - podstawową jednostkę przesyłania danych używaną w sieciach TCP/IP
  - operację trasowania (routingu), wykonywaną przez oprogramowanie IP, polegającą na wyborze trasy przesyłania danych
  - zbiór reguł służących do realizacji bezpołączeniowego dostarczania (sposób przetwarzania pakietów przez hosty i routery, komunikaty o błędach, warunki likwidowania pakietów)

Routing i routery

- Trasowanie (routing) – proces wybierania trasy, jaką należy przesłać pakiety
- Router (bramka, gateway) – komputer dokonujący takiego wyboru
  - W idealnej sytuacji oprogramowanie powinno brać pod uwagę np. obciążenie sieci, długość datagramu itp.; w praktyce zazwyczaj jednak brana jest pod uwagę tylko długość trasy

Etapy trasowania

- W trasowaniu (routingu) uczestniczą zarówno routery, jak i hosty
  - host generuje pakiety i decyduje, czy dostarczyć je bezpośrednio do adresata, czy przesłać do routera
  - router decyduje, czy przesłać pakiety bezpośrednio do adresata, czy do routera pośredniczącego (i ew. do którego routera, gdy jest ich kilka)

Rodzaje trasowania

- dostarczanie bezpośrednie
  - gdy wysyłający i odbiorca należą do tej samej sieci fizycznej: dostarczanie za pomocą ramek tej sieci.
- dostarczanie niebezpośrednie
  - nadawca musi zidentyfikować router do którego należy wysłać datagram, zaś router musi wysłać datagram w odpowiednim kierunku. Dostarczenie datagramu od nadawcy do routera odbywa się za pomocą sieci fizycznej

Informacja o trasach

- Informacja o trasach (czyli gdzie należy wysłać pakiet) może być:
  - statyczna
  - „wyuczona”
- Host lub router przechowuje informacje o trasach w swojej tablicy tras (tablicy routingu) - jest to tzw. *table-driven IP routing* – routing sterowany tablicami)

Tablice tras

- W tablicach tras pamiętane są przeważnie informacje o całych sieciach, a nie o poszczególnych komputerach
- Wybór trasy dokonywany jest na podstawie adresu IP (a przede wszystkim jego części *id_s* zawierającej numer sieci).
- Adresy wszystkich komputerów w danej sieci mają taki sam *id_s*, zatem umieszczenie w tablicy tras informacji o sieci jest wystarczające

Tablice tras – c.d.

- Tablica zawiera w większości wpisy postaci (S, R), gdzie S jest siecią docelową, a R – adresem IP „następnego etapu” *(next-hop router),* tj. najbliższego routera mogącego przesłać datagramy w kierunku sieci docelowej
- Jest to tzw. trasowanie etapami *(next-hop routing)*

Tablice tras – c.d.

- Konsekwencje wybierania tras jedynie na podstawie identyfikatora sieci docelowej:
  - w przypadku większości implementacji oznacza to, że pakiety z sieci A do sieci B będą przesyłane tą sama trasą, niezależnie od przepustowości i opóźnień
  - tylko ostatni router komunikuje się z adresatem datagramu, więc należy znaleźć sposób poinformowania nadawcy, że adresat nie istnieje lub nie działa

Tablice tras – c.d.

- każdy router wyznacza trasy niezależnie od innych, zatem pakiety wysyłane przez komputer A do komputera B mogą być przesyłane inną drogą niż wysyłane przez B do A

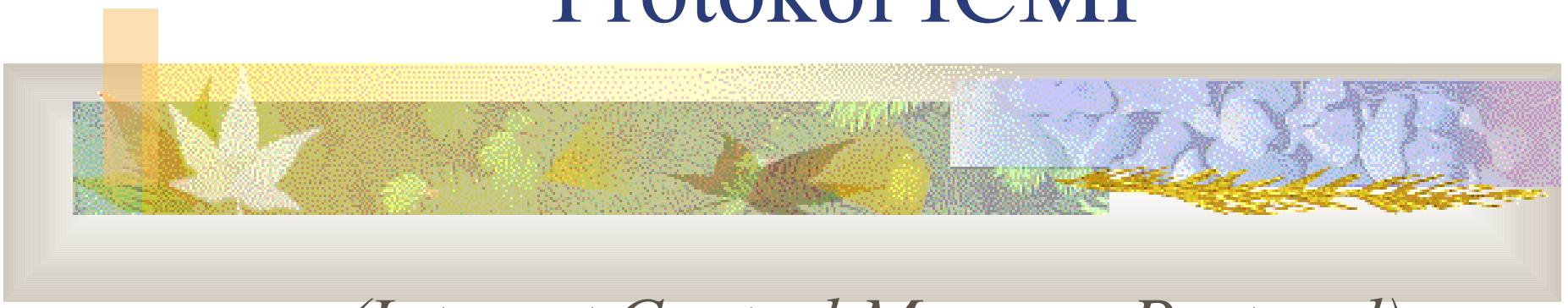
Wpisy w tablicach tras

- Tablica tras może zawierać następujące wpisy:
  - *identyfikator_sieci, dostarcz_bezpośrednio* – gdy posiadacz tablicy jest dołączony do danej sieci (dostarczanie bezpośrednie)
  - *adres_hosta, adres_nastepnego_etapu* – gdy pakiety przeznaczone dla danego hosta mają być przesyłane określoną trasą (trasa do hosta)
  - *identyfikator_sieci, adres_następnego_etapu* – trasa prowadząca do danej sieci (trasa do sieci)
  - *default, adres_następnego_etapu* – trasa domyślna, którą przesyła się wszystkie pakiety dla których nie określono innej trasy (trasa domyślna)

Algorytm trasowania

```
Algorytm WybierzTrase (datagram, tablica_tras):
na podstawie datagramu wyznacz IP adresata (D) i identyfikator
    sieci (N)
if (N zgodne z adresem którejś z bezpośrednio dołączonych
    sieci) then
        dostarcz datagram do D za pośrednictwem sieci
                fizycznej;
elsif (tablica zawiera trasę do hosta D) then
        wyślij datagram do routera podanego jako następny
                etap, używając sieci fizycznej;
elsif (tablica zawiera trasę do sieci N) then
        wyślij datagram do routera podanego jako następny
                etap, używając sieci fizycznej;
elsif (tablica zawiera trasę domyślną) then
        wyślij datagram do routera domyślnego, używając sieci
                fizycznej;
else zgłoś błąd trasowania
```

Protokół ICMP



(Internet Control Message Protocol)

Protokół IP - przypomnienie

- Protokół IP definiuje:
  - podstawową jednostkę przesyłania danych używaną w sieciach TCP/IP
  - operację trasowania (routingu), wykonywaną przez oprogramowanie IP, polegającą na wyborze trasy przesyłania danych
  - zbiór reguł służących do realizacji bezpołączeniowego dostarczania (sposób przetwarzania pakietów przez hosty i routery, komunikaty o błędach, warunki likwidowania pakietów)

Dostarczanie datagramu

- Datagram, którego nie można dostarczyć bezpośrednio, wędruje siecią od routera do routera, dopóki nie dotrze do takiego routera, który może go bezpośrednio dostarczyć do adresata

Sytuacje wyjątkowe

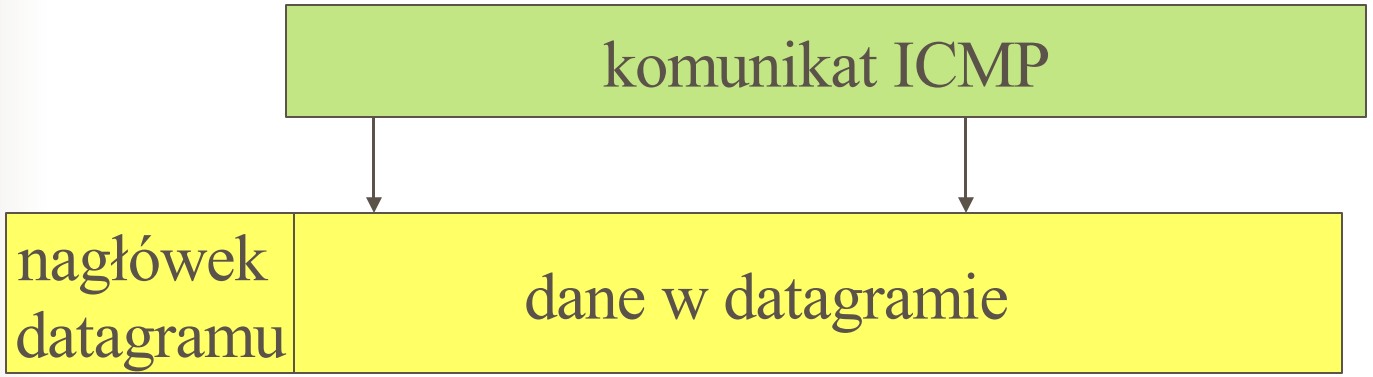
- Może okazać się, że router nie może przekierować ani dostarczyć datagramu:
  - błąd w tablicy tras (brak trasy do danej sieci/hosta i trasy domyślnej)
  - adresat nie istnieje lub nie działa
- W niektórych sytuacjach router musi zlikwidować otrzymany datagram:
  - przekroczony czas życia datagramu
  - przeciążenie routera

Reakcja na sytuacje wyjątkowe

- We wszystkich wymienionych wyżej sytuacjach router powinien poinformować nadawcę, że datagram nie zostanie dostarczony do adresata
- Samo IP nie zawiera żadnego pozwalającego na to mechanizmu
- Umożliwia to protokół ICMP – *Internet Control Message Protocol* - protokół komunikatów kontrolnych

Protokół ICMP

- IMCP jest wymaganą częścią IP
- Komunikaty ICMP są przesyłane siecią w części datagramu IP przeznaczonej na dane



Obsługa datagramów z ICMP

- Datagramy z komunikatami ICMP są obsługiwane w standardowy sposób. Jedyną różnicą jest, że w ich przypadku zajście „sytuacji wyjątkowych” nie powoduje generowania komunikatów o błędach

Rola ICMP

- Rolą komunikatów ICMP jest poinformowanie nadawcy datagramu o błędzie.
- Nadawca sam musi podjąć odpowiednie działania (komunikat ICMP może zawierać jednak pewne sugestie)

Format komunikatów ICMP

- Komunikat ICMP zawiera:
  - 8-bitowe pole typu i 8-bitowe pole kodu, informujące o rodzaju komunikatu
  - 16-bitową sumę kontrolną
  - komunikaty ICMP informujące o błędach zawierają ponadto pierwsze 64 bity datagramu który spowodował problem

Niektóre sytuacje obsługiwane przez ICMP

- Komunikaty ICMP przesyłane są w następujących sytuacjach:
  - przy testowaniu połączeń sieciowych
  - gdy router nie może dostarczyć datagramu
  - gdy router jest zbyt przeciążony, aby przyjąć nadchodzące datagramy
  - gdy router wykryje, że host przesyła datagramy nieoptymalną drogą

Niektóre sytuacje obsługiwane przez ICMP – c.d.

- gdy zostanie wykryte cykliczne przesyłanie datagramu lub przesyłanie go zbyt długą drogą
- w celu synchronizacji zegarów

Testowanie połączeń

- Diagnozowanie sieci może bazować na przesyłaniu komunikatów ICMP *echo request* i *echo reply* (prośba o „echo” i odpowiedź na tę prośbę)
- W wielu systemach poleceniem wykorzystującym te komunikaty jest `ping`

Testowanie połączeń - cd

Format komunikatu:

typ (0 lub 8)	kod	suma kontrolna
identyfikator		nr kolejny
opcjonalne dane		

- typ: prośba – 8, odpowiedź – 0
- identyfikator i nr kolejny umożliwiają przyporządkowanie odpowiedzi prośbom
- prośba zawiera opcjonalne dane; odpowiedź – kopię danych z prośby

Informacja o nieosiągalnym adresacie

- Gdy router nie może ani dostarczyć datagramu, ani przesłać go dalej, wysyła do nadawcy komunikat ICMP „adresat nieosiągalny” *(destination unreachable)*, a następnie likwiduje datagram

Informacja o nieosiągalnym adresacie – c.d

Format komunikatu:

typ (3)	kod (0-12)	suma kontrolna
nieużywane (musi być 0)		
nagłówek i pierwsze 64 bity datagramu IP		

- Komunikat zawiera początek straconego datagramu, co pozwala nadawcy określić jaki adresat jest nieosiągalny

Informacja o nieosiągalnym adresacie – c.d

- Niektóre używane kody:
  - 0 – sieć nieosiągalna *(network unreachable)*
  - 1 – host nieosiągalny *(host unreachable)*
  - 2 - protokół nieosiągalny *(protocol unreachable)*
  - 3 - port nieosiągalny *(port unreachable)*
  - 4 – konieczna fragmentacja przy ustawionym bicie „nie fragmentuj”
  - 5 – błąd trasowania wg nadawcy
  - 6 – nieznana sieć adresata

    itd...

Przeciążenia routerów

- Niekiedy router otrzymuje więcej datagramów, niż jest w stanie przetworzyć (stan ten nazywa się przeciążeniem – ang. *congestion*)
- Przeciążenie może wystąpić np. gdy wiele komputerów przesyła dane przez ten sam router, lub gdy jeden komputer generuje dane zbyt prędko
- Przychodzące datagramy są kolejkowane

Przeciążenia routerów – c.d.

- Jeśli przysyłanie do routera nadmiernej ilości datagramów trwa zbyt długo, to kolejka nie może ich pomieścić
- W takiej sytuacji przychodzące datagramy są likwidowane, a router wysyła do ich nadawcy (-ów) komunikat ICMP *source quench* – prośbę o zredukowanie nadawania
- w odpowiedzi nadawca powinien zmniejszyć ilość wysyłanych danych

Przeciążenia routerów – c.d.

Format komunikatu:

typ (4)	kod (0)	suma kontrolna
nieużywane (musi być 0)		
nagłówek i pierwsze 64 bity datagramu IP		

- dzięki dołączeniu początku datagramu nadawca wie, które dane nie zostały przesłane do adresata

Przeciążenia routerów – c.d.

- Zwykle routery generują po jednym komunikacie dla każdego likwidowanego datagramu
- Możliwe jest też śledzenie przychodzących pakietów i wysyłanie komunikatu do najbardziej aktywnego nadawcy
- Routery mogą generować komunikaty ICMP już wtedy, gdy ich kolejki są długie, ale jeszcze nie przepełnione

Prośba o zmianę trasy

- Zakłada się, że routery posiadają pełną informację o trasach, zaś hosty startują z minimalną „wiedzą” (trasa domyślna, dostarczanie bezpośrednie), a następnie zdobywają dalsze informacje od routerów

Prośba o zmianę trasy – c.d.

- Gdy router (będący w tej samej sieci co nadawca) wykryje, że nadawca wysyła datagramy nieoptymalną drogą, wysyła do niego komunikat „prośba o zmianę trasy” (ICMP *redirect*) i wysyła datagram do adresata
- W odpowiedzi host modyfikuje swoją tablicę tras
- Nie rozwiązuje to wszystkich problemów nieoptymalnego trasowania, gdyż jest ograniczone do jednej sieci fizycznej

Prośba o zmianę trasy – c.d.

Format komunikatu:

typ (5)	kod (0-3)	suma kontrolna
adres IP routera		
nagłówek i pierwsze 64 bity datagramu IP		

- komunikat zawiera adres IP routera, stanowiącego „optymalny” „następny etap” dla datagramu, którego początek jest zapisany w komunikacie
- pole kodu określa, jak należy interpretować adres docelowy zapisany w datagramie (0 – sieć, 1 – host, 2 – typ obsługi i sieć, 3 – typ obsługi i host)

Prośba o zmianę trasy – c.d.

- Komunikaty ICMP *redirect* używane są tylko do komunikacji routerów z hostami
- Same routery używają do komunikacji między sobą innych protokołów

protokoły komunikacji między routerami zostaną omówione później

Wykrywanie cyklicznych lub zbyt długich tras

- W sytuacji, gdy router musi zlikwidować datagram, ponieważ jego pole TTL ma wartość 0, do nadawcy datagramu wysyłany jest komunikat ICMP „przekroczenie czasu” *(time exceeded)*
- podobny komunikat wysyłany jest, gdy host nie otrzyma wszystkich fragmentów datagramu w odpowiednim czasie od przybycia pierwszego z otrzymanych fragmentów

Wykrywanie cyklicznych lub zbyt długich tras – c.d.

- Format komunikatu:

typ (11)	kod (0 lub 1)	suma kontrolna
nieużywane (musi być 0)		
nagłówek i pierwsze 64 bity datagramu IP		

  - kod 0 – przekroczony czas życia datagamu
  - kod 1 – fragmenty nie dotarły w przewidzianym czasie

Powiadamianie o innych problemach

- W przypadku, gdy router ma z datagramem inny problem niż przedstawione wcześniej (np. datagram ma niepoprawny nagłówek), wysyła do nadawcy komunikat o błędzie *(ICMP parameter problem)*

Powiadamianie o innych problemach – c.d.

- Format komunikatu:

typ (12)	kod (0 lub 1)	suma kontrolna
wskaźnik	nieużywane (musi być 0)	
nagłówek i pierwsze 64 bity datagramu IP		

  - Pole *wskaźnik* określa, który oktet w datagramie spowodował problem
  - kod 1 – brakuje pewnej wymaganej opcji; w tym przypadku pole *wskaźnik* nie jest używane

Problemy adresowania IP

Adresowanie IP

- W oryginalnym schemacie adresowania IP każda sieć fizyczna ma przypisany unikalny numer sieci, a każdy host ma adres IP zawierający numer sieci w której się znajduje

Adresowanie IP – c.d.

- Zaleta powyższego schematu:
  - mniejsze tablice routingu
  - poszczególne ośrodki mogą dowolnie modyfikować adresy i trasy, dopóki pozostaje to niewidoczne dla „reszty świata”
    - wszystkie hosty i routery w tym ośrodku muszą akceptować taki schemat adresowania
    - reszta Internetu powinna móc traktować adresy wg standardowego schematu

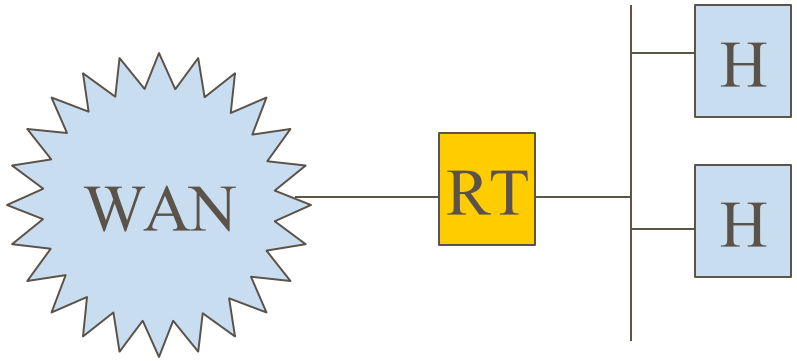
Problem z adresowaniem IP

- Zwiększanie się Internetu spowodowało problemy z adresowaniem:
  - rosnące tablice routingu
    - duże obciążenie sieci z powodu wymiany informacji przez routery
    - konieczność wykonywania przez routery dużej ilości obliczeń podczas aktualizowania tras
  - wyczerpywanie się przestrzeni adresowej
    - oryginalny schemat adresowania IP (klasy) jest niewystarczający (zbyt mało numerów dla niewielkich sieci)

Możliwe rozwiązania

- Ten sam numer sieci (przedrostek sieciowy w IP) jest przypisywany kilku sieciom fizycznym
  - routery „przezroczyste”
  - proxy ARP
  - adresowanie w podsieciach (subnetting)
  - NAT (Network Address Translation)
- Protokół IPv6

Routery „przezroczyste”



- Sieć rozległa i sieć lokalna używają adresów o tym samym prefiksie sieciowym
- Sieć lokalna połączona jest z siecią rozległą tzw. routerem przezroczystym (*transparent router*), niewidocznym dla komputerów w sieci
- Router przezroczysty przekazuje do sieci WAN pakiety od komputerów z sieci lokalnej oraz odbiera z WAN-u pakiety dla tych komputerów. Może jednak nie pełnić wszystkich funkcji routera

Proxy ARP

- Dwie sieci fizyczne (A,B) mają ten sam przedrostek sieciowy adresów IP
  - Router łączący te sieci pozwala komputerom komunikować się tak, jakby była to jedna sieć – w odpowiedzi na zapytania ARP pochodzące z sieci B i dotyczące maszyn z A odpowiada swoim adresem fizycznym, a otrzymane w ten sposób datagramy przesyła do odpowiednich komputerów w sieci A
  - Postępowanie dla przesyłu z sieci A do B jest analogiczne
- Rozwiązanie tylko dla sieci stosujących ARP; niewykonalne przy ARP z kontrolą spoofingu

Podsieci (subnetting)

- Rozwiązanie polegające na zmianie interpretacji adresu IP:
  - w części adresu przeznaczonej standardowo na numer hosta wyróżnia się dwie części: numer podsieci i numer hosta
  - o sposobie podziału informuje maska podsieci

Podsieci – c.d.

- Rozwiązanie zestandaryzowane
  - standard zabrania przypisywania sieciom fizycznym adresów, w których:
    - wszystkie bity w numerze podsieci są równe 0
    - wszystkie bity w numerze podsieci są równe 1

    (praktyka jest często inna od standardu)
  - bity adresu przeznaczone na nr sieci + podsieci nie muszą być ciągłym fragmentem adresu
  - każda sieć fizyczna może mieć inną maskę
    - standard zaleca, żeby maska była ciągła i jednakowa dla wszystkich sieci współdzielących dany przedrostek sieciowy adresu IP

Trasowanie w podsieciach

- Standardowy algorytm routingu musi zostać zmodyfikowany tak, aby uwzględniał podsieci
  - tablica tras zawiera trójki *(nr_sieci, maska_sieci, adres_IP_routera)*
  - wybór trasy dokonywany jest z uwzględnieniem maski
  - wszystkie komputery w danej sieci muszą używać zmodyfikowanego algorytmu
- możliwe jest zastosowanie podsieci tylko lokalnie i ukrycie tego faktu przed siecią rozległą

Translacja adresów - NAT

- NAT = *Network Address Translation*
- Polega na „podmianie” adresu nadawcy w datagramie
- Podmiany dokonuje router przekazujący ten datagram
- Przykład translacji adresów – tzw. *IP masquerading*

IP masquerading (maskarada)

- Komputerom w sieci lokalnej przypisujemy tzw. nierutowalne (prywatne) adresy IP:
  - klasa A: 10.0.0.0 - 10.255.255.255
  - klasa B: 172.16.0.0 - 172.31.0.0
  - klasa C: 192.168.0.0 - 192.168.255.0
- Router ma przypisany „publiczny” adres IP
- Router zastępuje w datagramach adresy nadawców z sieci lokalnej swoim adresem IP, a przychodzące w odpowiedzi pakiety rozsyła odpowiednim komputerom w sieci lokalnej

IP masquerading – c.d.

- Cały ruch z sieci lokalnej widziany jest jako wychodzący z jednego komputera (routera)
- Komputery w sieci lokalnej są ukryte przed „światem”, nie można więc zaadresować pakietów bezpośrednio do nich

Protokół IPv6

nowa wersja protokołu IP

Protokół IPv6

- Wersja protokołu IP omówiona wcześniej to wersja 4 (IPv4)
- Opracowanie nowej wersji (6, oznaczanej jako IPv6, IPng) zostało spowodowane m.in. przez wyczerpywanie się przestrzeni adresowej

Protokół IPv6 – c.d.

- Cechy IPv6 analogiczne do IPv4:
  - protokół bezpołączeniowy
  - umożliwia nadawcy wybieranie rozmiaru datagramu
  - nagłówek datagramu zawiera adres IP nadawcy i odbiorcy
  - adres odbiorcy służy do wyznaczania trasy
  - jedno z pól nagłówka ogranicza liczbę routerów, przez które może przejść datagram
  - zachowana została większość rozwiązań związanych z opcjami IPv4, w tym związanych z fragmentacją i trasowaniem wg nadawcy

Protokół IPv6 – c.d.

- Nowe cechy IPv6:
  - dłuższe adresy (128-bitowe zamiast 32-bitowe)
  - elastyczny format nagłówka
  - ulepszone opcje IP
  - wsparcie dla rezerwowania zasobów
    - można ustanowić ścieżkę wysokiej jakości przez sieci bazowe i powiązać datagramy z tą ścieżką; przydatne dla aplikacji multimedialnych
  - zapewnienie rozszerzalności protokołu

Adresy IPv6

- Adres 128-bitowy (ponad $3.4 \cdot 10^{38}$ adresów)
  - *gdyby adresy były przypisywane z prędkością milion adresów na mikrosekundę, to przypisanie wszystkich zajęłoby około 20 lat*
- Nie ma klas, podział na prefiks i sufiks może przebiegać w dowolnym miejscu i nie można go wyznaczyć na podstawie samego adresu

Adresy IPv6 – c.d.

- Zestaw adresów specjalnego przeznaczenia bardzo się różni od IPv4:
  - nie ma rozgłoszenia skierowanego do danej sieci
  - każdy adres należy do jednego z trzech podstawowych typów:
    - adres jednostkowy
    - adres rozsyłania grupowego
    - adres grona

Adresy IPv6 – c.d.

- Adres jednostkowy –
  - datagram wysyłany pod ten adres jest przesyłany najkrótszą trasą do danego komputera
- Adres rozsyłania grupowego –
  - odpowiada zbiorowi komputerów, które mogą się znajdować w różnych miejscach sieci
  - przynależność do tego zbioru można zmieniać w dowolnym momencie
  - datagram wysyłany pod taki adres jest dostarczany do wszystkich członków grupy

Adresy IPv6 – c.d.

- Adres grona -
  - adres odpowiadający zbiorowi komputerów mających pewien wspólny prefiks adresu (np. znajdują się one w jednym miejscu)
  - datagram dostarczany jest najkrótszą ścieżką do tego miejsca, a następnie dostarczany jednemu z członków grupy
  - grona stosuje się z powodu konieczności zapewnienia repliki usługi

Adresy IPv6 – c.d.

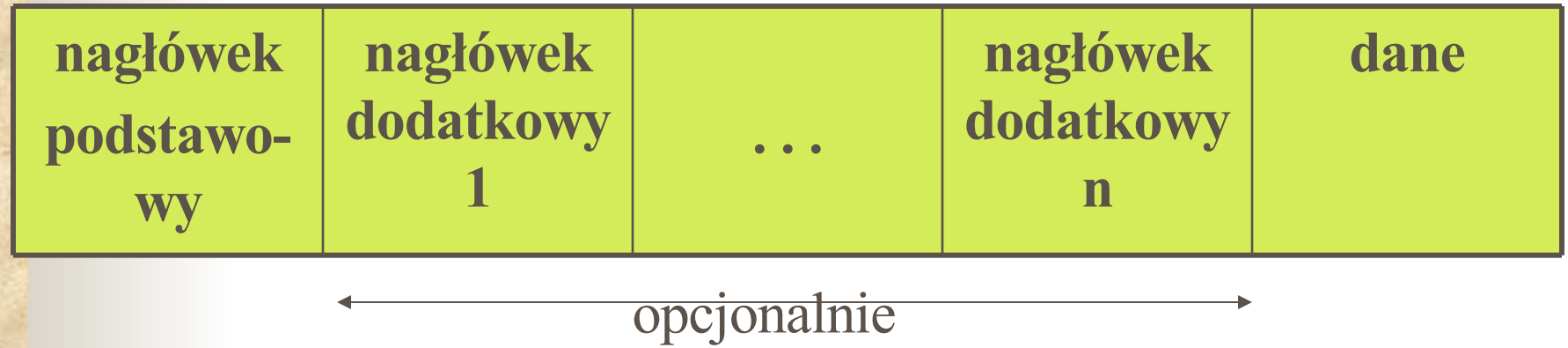
- Format adresów umożliwia adresowanie hierarchiczne, np:

typ adresu	provider ID	subscriber ID	subnet ID	node ID

- Istnieje możliwość odwzorowania adresu IPv4 na adres IPv6 (96 bitów wypełnionych zerami, dalej – 32 bity jak w adresie IPv4)

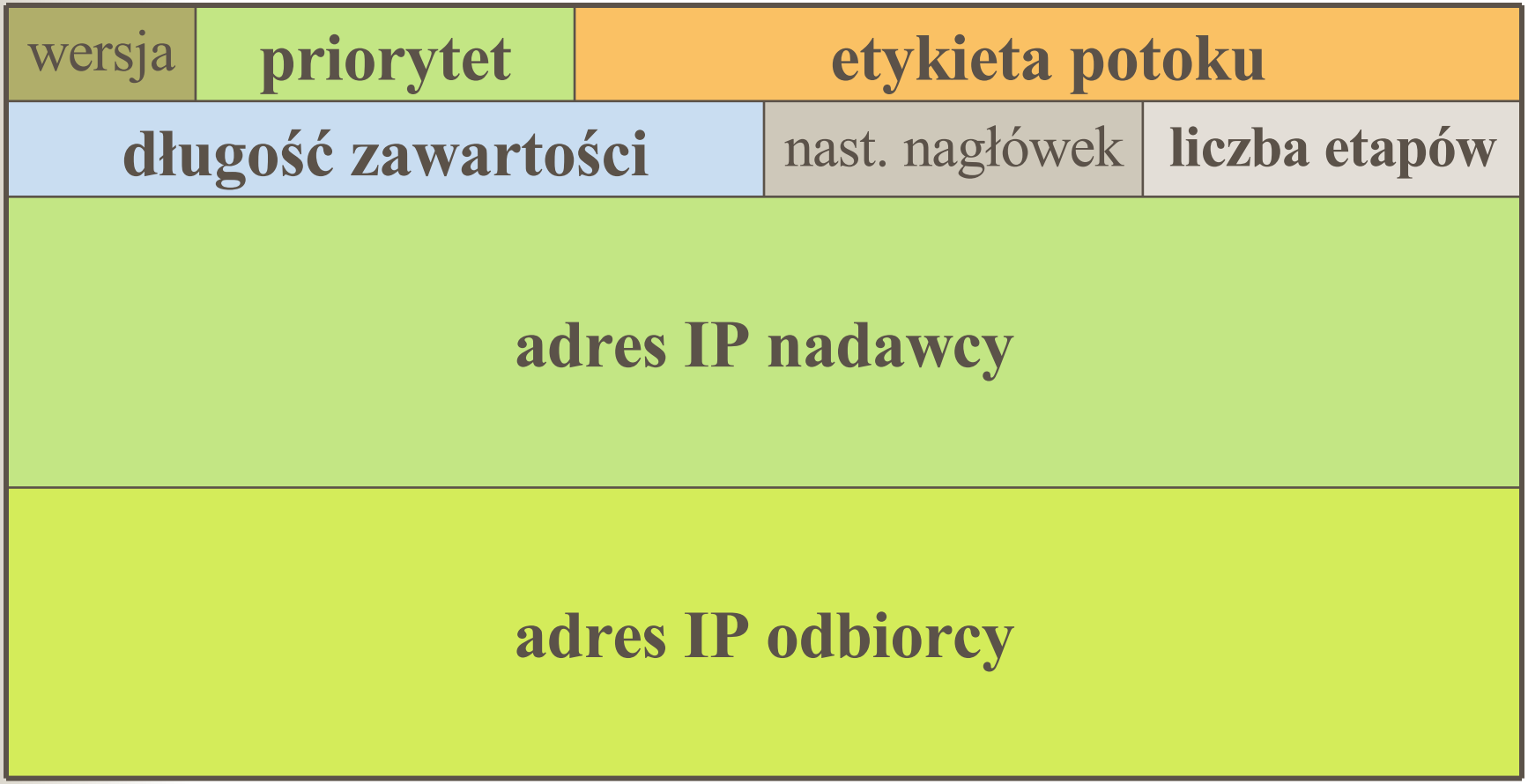
Datagram IPv6

- Datagram IPv6 zaczyna się od nagłówka podstawowego, po którym następuje zero lub więcej nagłówków dodatkowych, po których następują dane



Nagłówki dodatkowe mogą być różnych rozmiarów

Datagram IPv6: nagłówek podstawowy



Nagłówek podstawowy – c.d.

- **wersja** – wersja protokołu IP (tu 6)
- **priorytet** – określenie priorytetu datagramu
- **długość zawartości** – określa (w oktetach) rozmiar przenoszonych danych (bez nagłówków). Datagram może zawierać do 64 kilobajtów danych
- **liczba etapów** – odpowiada polu czas życia w datagramie IPv4.
  - Różnica – w IPv4 czas życia był traktowany jako kombinacja czasu i liczby etapów; tu jest to dokładnie liczba etapów (routerów przez które przechodzi datagram)

- Rozmiar nagłówka podstawowego – 40 oktetów

Datagram IPv6: nagłówki dodatkowe

- Dodatkowe nagłówki pełnią rolę podobną do opcji IPv4 – nadawca może zdecydować, jakie dołączyć, a jakich nie
- Każdy z nagłówków – podstawowy i dodatkowe – zawiera pole **następny nagłówek**, pozwalające określić rodzaj kolejnego nagłówka lub typ danych przenoszonych w datagramie, jeśli następny nagłówek nie istnieje

IPv6: fragmentacja datagramów

- Datagramy IPv6 są fragmentowane z analogicznych powodów jak datagramy IPv4
- Połączenie fragmentów odbywa się u ostatecznego odbiorcy
- Datagramy będące fragmentami mają dodatkowy nagłówek fragmentacji