Sieci komputerowe

Sławomir Samolej
ssamolej.kia.prz.edu.pl
ssamolej@kia.prz.edu.pl

Definicja

Sieć komputerowa to zbiór niezależnych komputerów, które mogą się ze sobą komunikować.

Medium komunikacyjnym mogą być przewody miedziane, światłowody lub fale elektromagnetyczne (radio, mikrofale, podczerwień, łączność satelitarna).

Podstawowe właściwości

- Sieć komputerowa służy współużywania zasobów
- Schematy wymiany komunikacji:
  - Klient-serwer
  - Każdy-z-każdym (ang. peer-to-peer)
- Sieć oferuje możliwość obliczeń współbieżnych i rozproszonych
- Sieć jest globalnym medium komunikacji (WWW, poczta, VoIP, IoT)
- Zasady konstrukcji urządzeń sieciowych i protokoły wymiany informacji są unormowane w dokuymentach (IEEE, ISO, RFC)

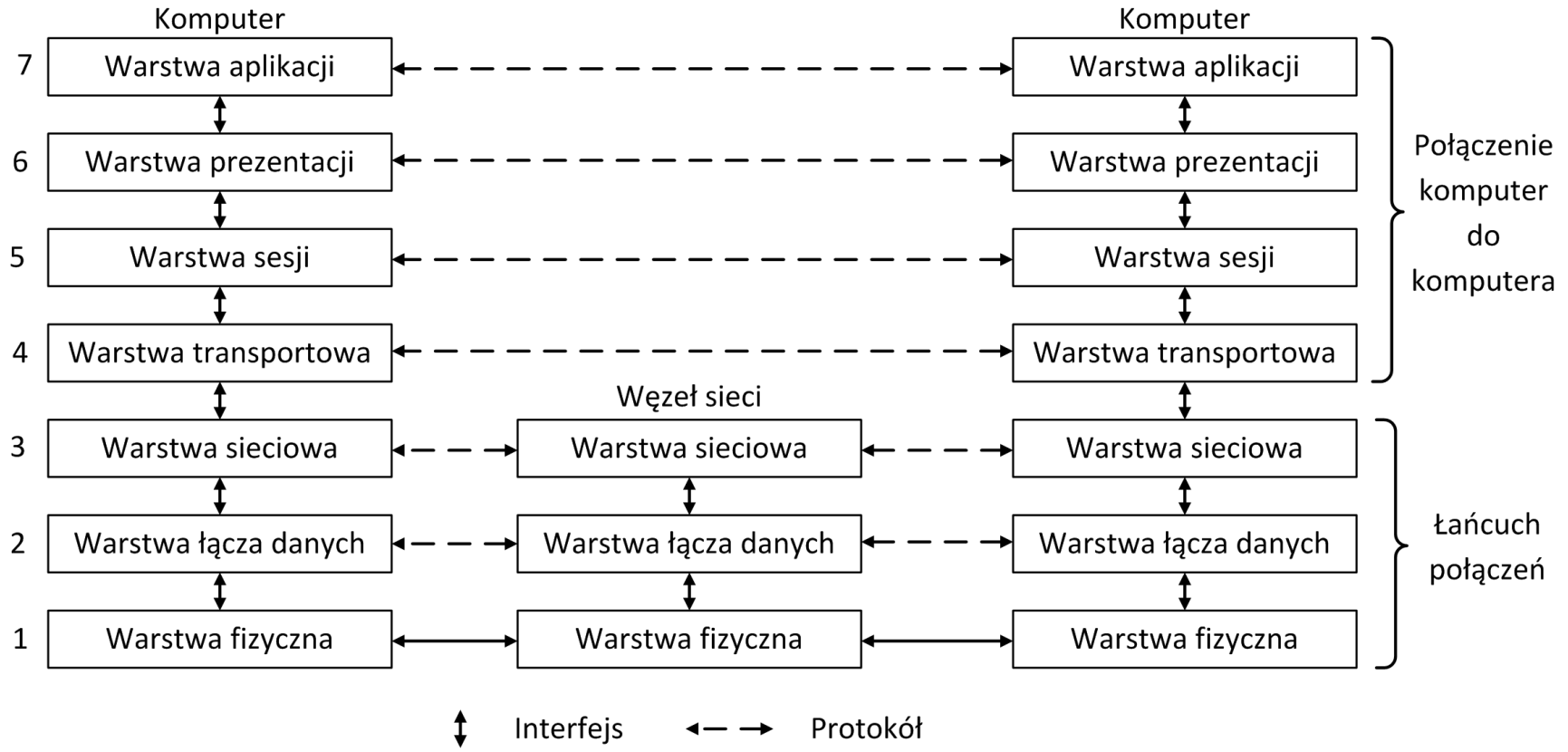
Historia sieci komputerowych

- Pierwsze sieci komputerowe miały charakter rozległy i łączyły „duże komputery” za pomocą dostępnych łączy telekomunikacyjnych
- W latach 70-tych zaczęto konstruować sieci łączące komputery osobiste w celu współdzielenia np. drukarek
- Z czasem jedne i drugie sieci zlały się w sieć globalną
- Obecnie sieć komputerowa przejmuje wszystkie strumienie telekomunikacyjne (np. telefon, telewizja, radio, VoD, komunikatory) i staje się dominującym medium wymiany informacji

Klasyfikacja sieci

Odległość między węzłami	*Węzły położone w tym samym*	*Przykład*
1 m	metrze kwadratowym	sieć osobista
10 m	pomieszczeniu	sieć lokalna
100 m	budynku	
1 km	grupie budynków	
10 km	mieście	sieć miejska
100 km	kraju	sieć rozległa
1000 km	kontynencie	
10 000 km	planecie	Internet

Model warstwowy sieci komputerowych ISO-OSI



Zalety warstwowego opisu sieci

- Komunikacja w sieci jest zorganizowana w postaci stosu **warstw**
- Zadaniem kolejnej warstwy jest dostarczenie warstwom wyższym określonych **usług** bez podawania informacji, jak dane usługi zostały zaimplementowane
- Zmiana implementacji jednej z warstw nie powinna mieć żadnego wpływu na pracę pozostałych warstw
- Pozwala to na ewolucyjną wymianą oprogramowania i sprzętu przy zachowaniu ciągłości działania infrastruktury komunikacji sieciowej jako całości
- Istotną właściwością takiego podejścia jest to, że podczas komunikacji wymiana informacji następuje pomiędzy odpowiadającymi sobie warstwami
- W rzeczywistości każda warstwa przesyła informację do warstwy znajdującej się poniżej, uzupełniając je odpowiednimi informacjami sterującymi.

Warstw fizyczna

- Warstwa fizyczna nazywana warstwą sprzętową zajmuje się fizycznym przesyłaniem bitów w kanale informacyjnym.
- Jej zadaniem jest przesłanie kolejnych bitów danych pomiędzy komputerami tworzącymi sieć lokalną.
- Na poziomie tej warstwy ustala się poziomy napięć w kablu miedzianym, kolory i intensywność światła w światłowodzie, częstotliwości i metody modulacji fal elektromagnetycznych w łączności bezprzewodowej, a także parametry czasowe przesyłanych sygnałów.
- Warstwa ta definiuje również standardy złączy, interfejsy mechaniczne i elektryczne, zgodnie z którymi mają pracować fizyczne urządzenia sieciowe.

Warstwa łącza danych

- Warstwa łącza danych odpowiada za niezawodne przesłanie danych pomiędzy komputerami tworzącymi sieć lokalną.
- W tym celu dane są dzielone na fragmenty zwane **ramkami**. Każda ramka jest przesyłana osobno.
- W przesyłaniu ramek stosuje się matematyczne metody wykrywania błędów (np. sumy kontrolne), techniki potwierdzania, że ramka dotarła oraz retransmisję uszkodzonych ramek.
- W tej warstwie mogą zostać również zdefiniowane techniki kontroli przepływu, czyli metody powiadamiania nadawcy, że nadaje zbyt szybko, aby można było bez utraty odbierać jego dane.

Warstwa sieciowa

- Warstwa sieciowa jest odpowiedzialna za przesłanie pakietów danych pomiędzy dwoma komputerami, które potencjalnie mogą się znaleźć w dowolnych miejscach na Ziemi
- Na poziomie tej warstwy są definiowane techniki wyznaczania tras oraz kontroli przepływu w sieciach rozległych
- Na tym poziomie muszą być również rozstrzygnięte problemy przesłania pakietu danych z zastosowaniem sieci o różnej architekturze, formacie i szybkości przesyłania informacji
- Warstwa nie zapewnia niezawodnego przesyłania danych

Warstwa transportowa

- Na poziomie warstwy transportowej dane otrzymywane z warstwy wyższej są formułowane w pakiety.
- Warstwa ta jest odpowiedzialna za niezawodny przesył tych pakietów pomiędzy dwoma komputerami znajdującymi się w dowolnym miejscu na Ziemi.
- W tym celu są sformułowane specjalne protokoły wymiany danych pomiędzy komputerami znajdującymi się potencjalnie w dwu różnych sieciach komputerowych.

Warstwa sesji

- Warstwa sesji pozwala na ustanowienie połączenia pomiędzy aplikacjami pracującymi na komunikujących się komputerach.
- Zapewnia utrzymanie połączenia lub jego wznowienie, jeśli zostało przerwane.

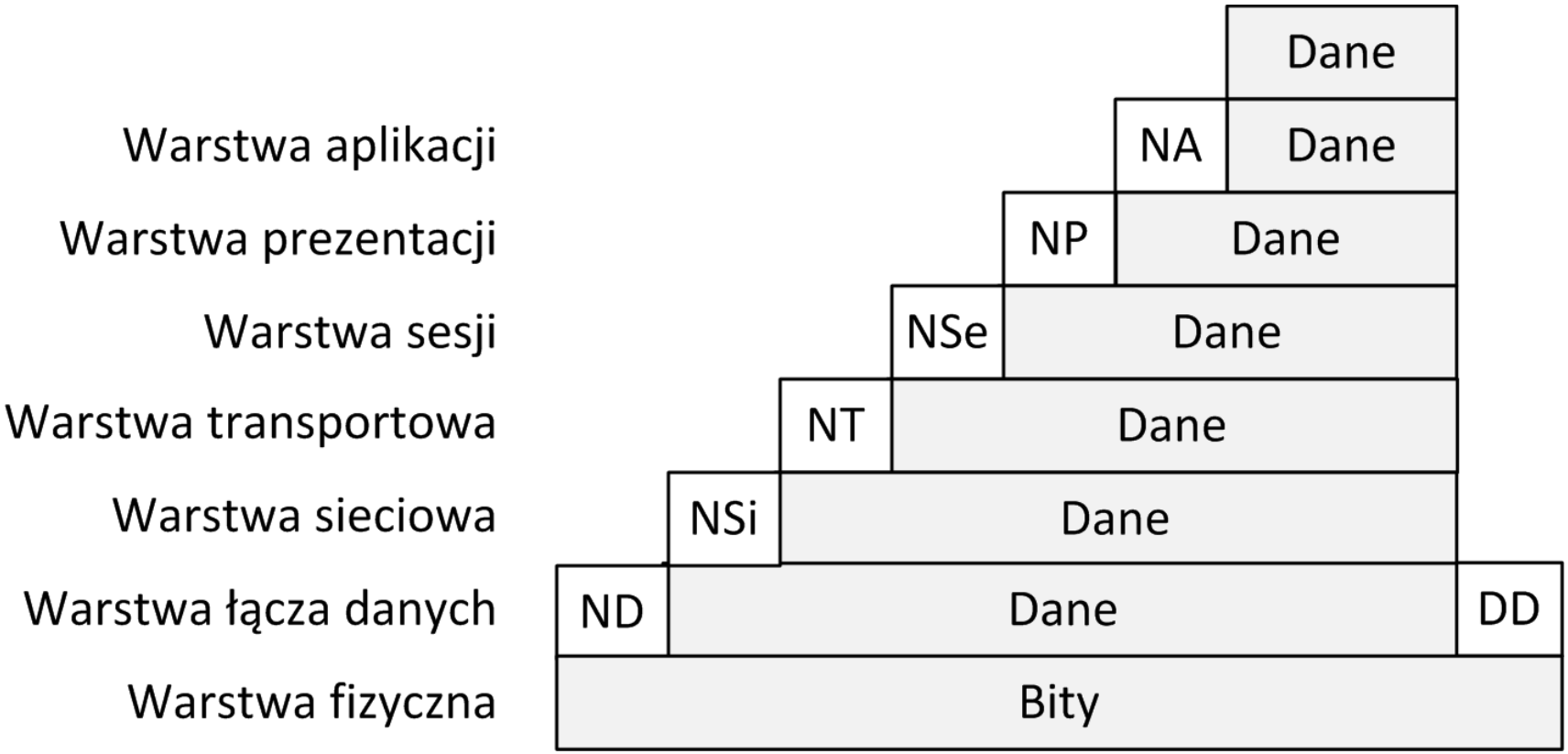
Warstwa prezentacji

- Warstwa prezentacji odpowiada za konwersję (jeśli jest potrzebna) sposobu reprezentacji danych.
- Warstwa udostępnia mechanizmy uniwersalnego kodowania danych dla transportu w sieci oraz możliwość „powracania” do kodowania charakterystycznego dla danej architektury komputera.

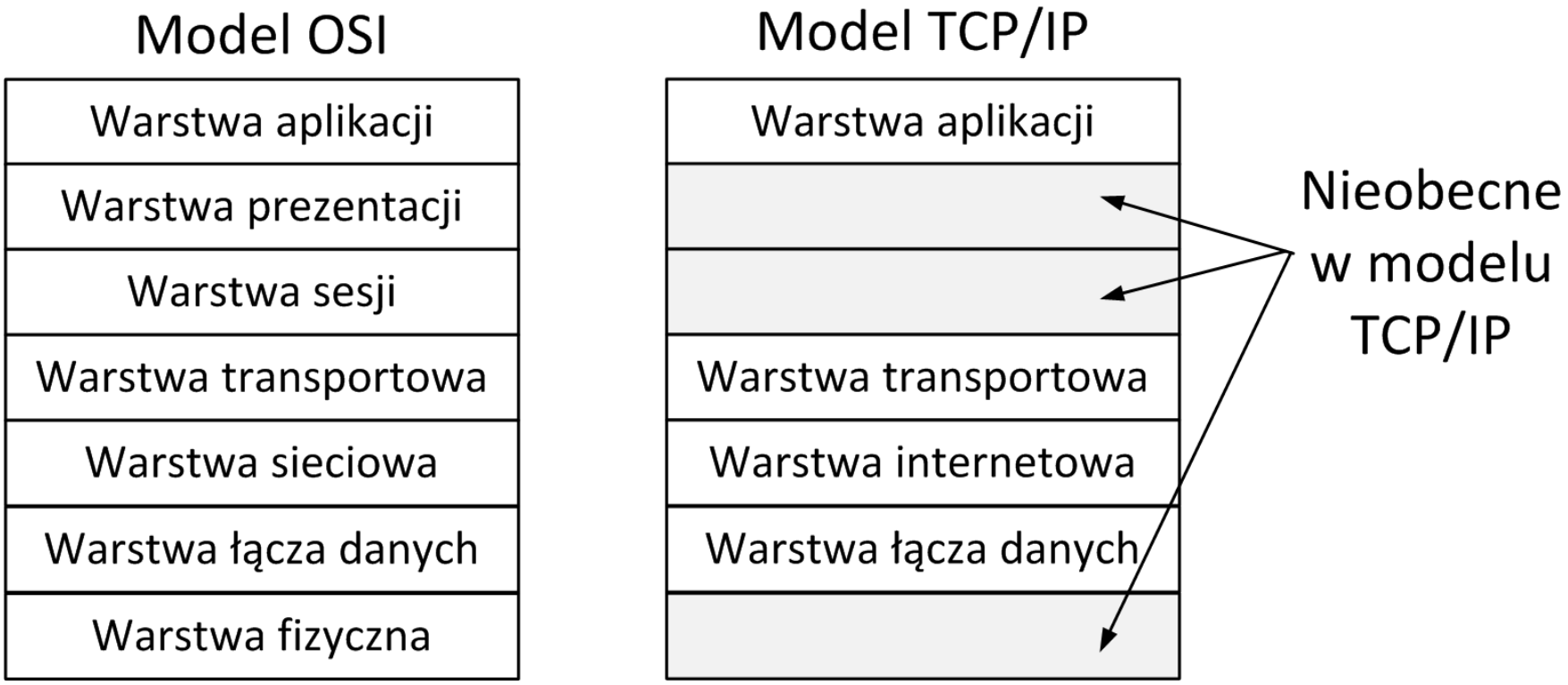
Warstwa aplikacji

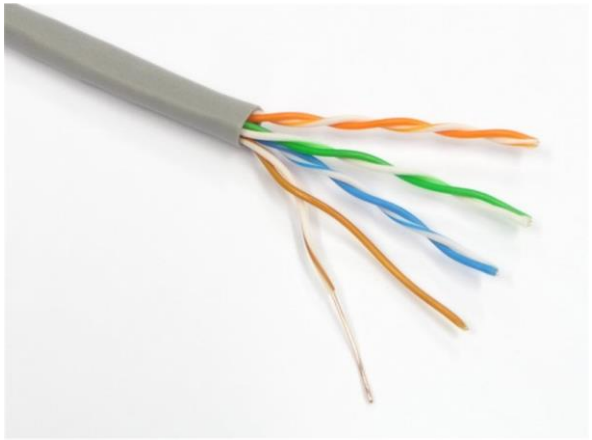
- Na poziomie warstwy aplikacji sa¸ zdefiniowane protokoły sieciowe, którymi posługują się programy użytkowników.
- Przykładami takich protokołów są HTTP (ang. HyperText Transfer Protocol) do przesyłania zawartości stron WWW (ang. World Wide Web) czy SMTP (ang. Simple Mail Transfer Protocol) do przesyłania wiadomości pocztowych.
- Inne protokoły umożliwiają przesyłanie plików, list dyskusyjnych itp.
- Za tą warstwą kryją się również po prostu programy użytkowników korzystające z łączności sieciowej.

Opakowywanie danych



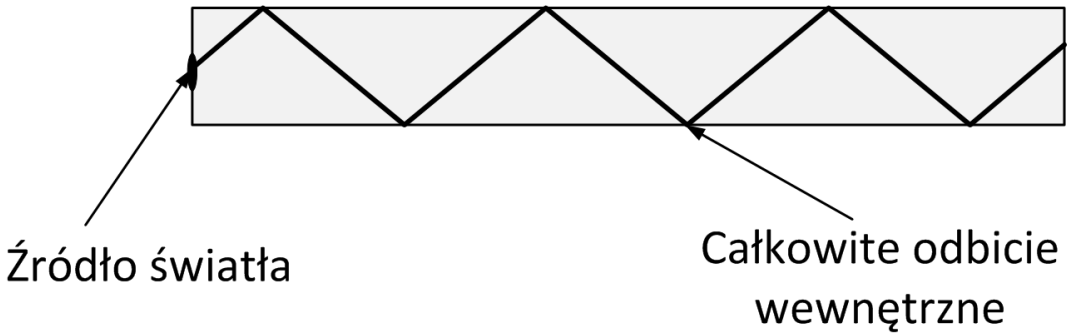
Model TCP/IP


Model OSI
Warstwa aplikacji
Warstwa prezentacji
Warstwa sesji
Warstwa transportowa
Warstwa sieciowa
Warstwa łącza danych
Warstwa fizyczna
Model TCP/IP
Warstwa aplikacji
Warstwa transportowa
Warstwa internetowa
Warstwa łącza danych
Nieobecne w modelu TCP/IP



Media - Skrętka

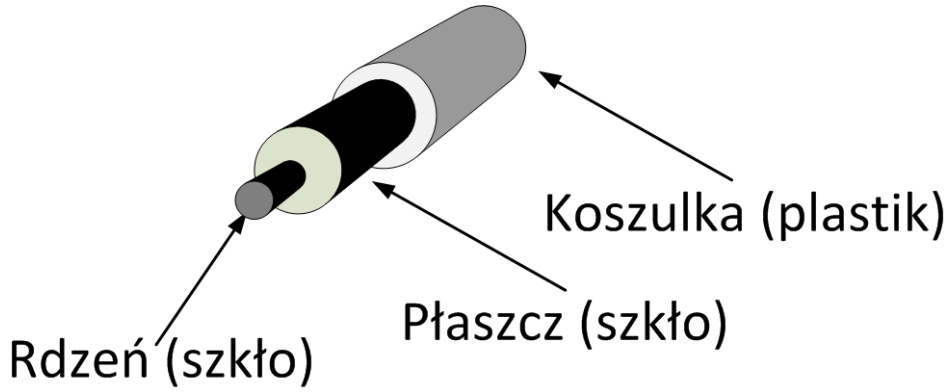
- Skrętka jest nadal jednym z najczęściej stosowanych nośników transmisji, zwłaszcza w sieciach lokalnych. Składa się z dwu izolowanych przewodów lub drutów miedzianych o średnicy ok. 1 mm skręconych ze sobą w helisę, podobnie jak cząsteczka DNA. Skręcanie przewodów jest niezbędne, ponieważ wygłusza fale elektromagnetyczne wytwarzane oraz odbierane przez parę kabli.
- Sygnał przesyłany przez parę kabli jest zwykle kodowany przez zmianę różnicy napięć pomiędzy przewodami. Obecnie najczęściej stosowanym typem skrętki jest kabel kategorii 5. (CAT 5). Składa się on z dwu izolowanych przewodów lekko skręconych, zwykle grupowanych po cztery pary we wspólnej powłoce



Wewnętrzne odbicie

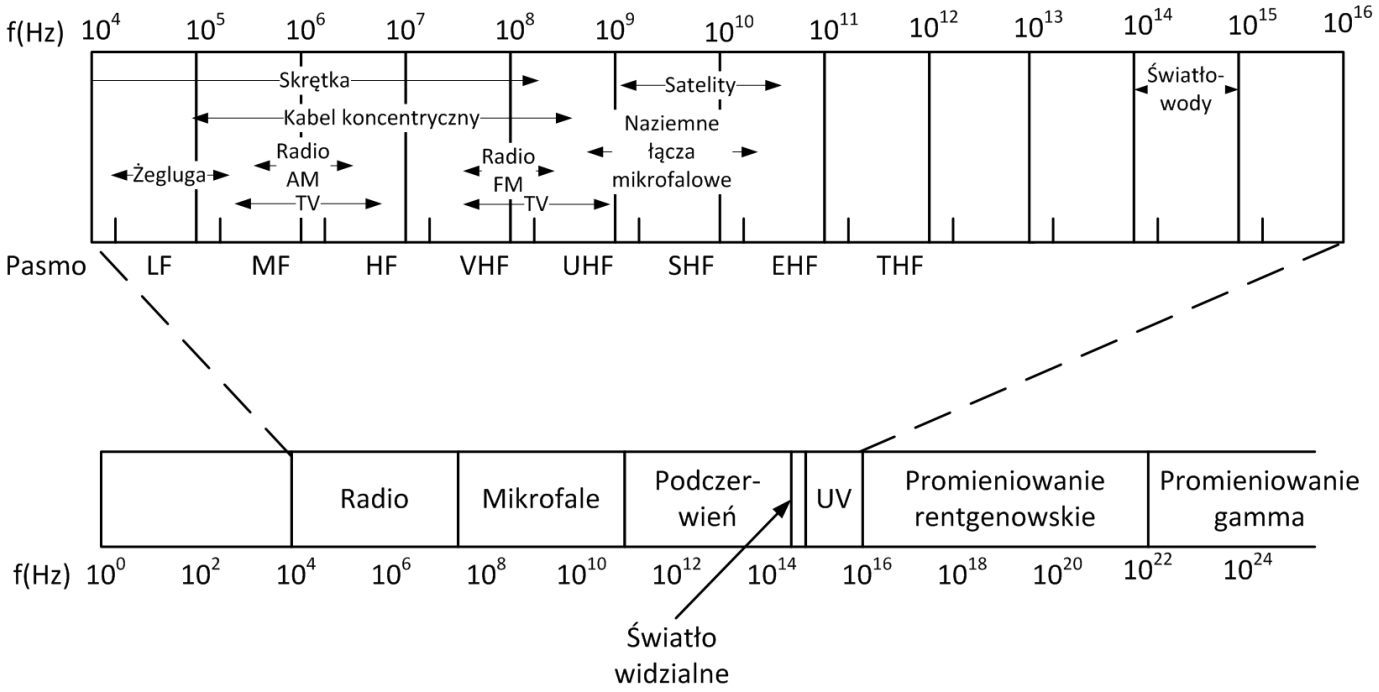
- System transmisji światłowodowej składa się z trzech podstawowych składników: źródła światła, medium transmisyjnego oraz detektora.
- Impuls światła oznacza sygnał o wartości „1”, brak światła to bit „0”. Jeżeli medium transmisyjnym jest odpowiednie ultracienkie przejrzyste włókno szklane i promień światła wpada do niego pod odpowiednim kątem, to następuje w nim zjawisko całkowitego odbicia wewnętrznego
- Promień światła może być w ten sposób przenoszony na odległość wielu kilometrów praktycznie bez strat
- Jeśli włókno światłowodowe umożliwia wprowadzanie promieni pod wieloma kątami, mówi się, że jest to światłowód wielomodowy.
- Inny rodzaj światłowodu o grubości zredukowanej do kilku długości fali świetlnej zachowuje się jak falowód. Umożliwia on wprowadzenie jednego promienia świetlnego poruszającego się w linii prostej. Taki światłowód jest nazywany jednomodowym.

Media - Kabel światłowodowy



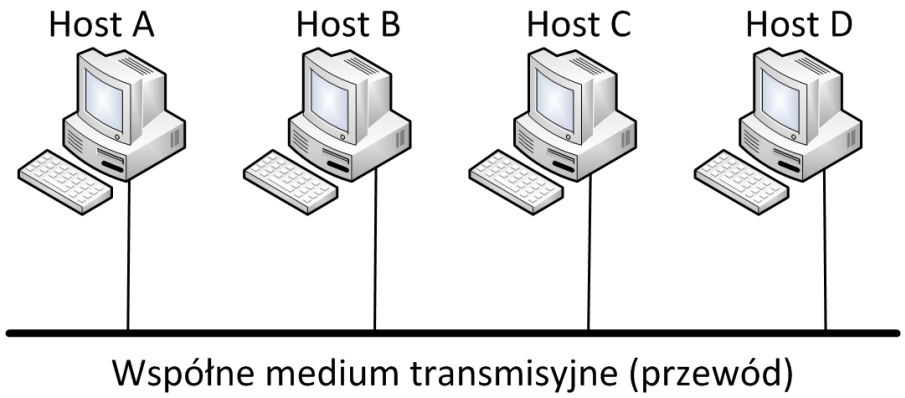
- Kabel światłowodowy składa się z rdzenia wykonanego ze szkła otoczonego przez płaszcz ze szkła o innym współczynniku załamania niż w rdzeniu, co powoduje, że światło pozostaje w rdzeniu.
- Koszulka z tworzywa sztucznego chroni płaszcz.
- Włókna światłowodowe łączy się wiązki chronione dodatkową otuliną zewnętrzną. Emiterami światła dla światłowodów są diody świecące lub lasery, odbiornikami – fotodiody.

Media - widmo elektromagnetyczne



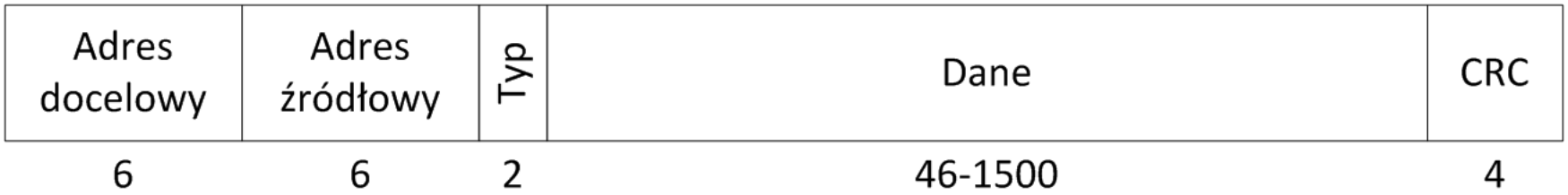
- Systematycznie opracowywane są nowe standardy łączności cyfrowej z zastosowaniem fal elektromagnetycznych.
- Są rozwiązania oferujące połączenia cyfrowe z zastosowaniem
  - Fal radiowych
  - Światła
  - Mikrofal

Pierwsza struktura Ethernet



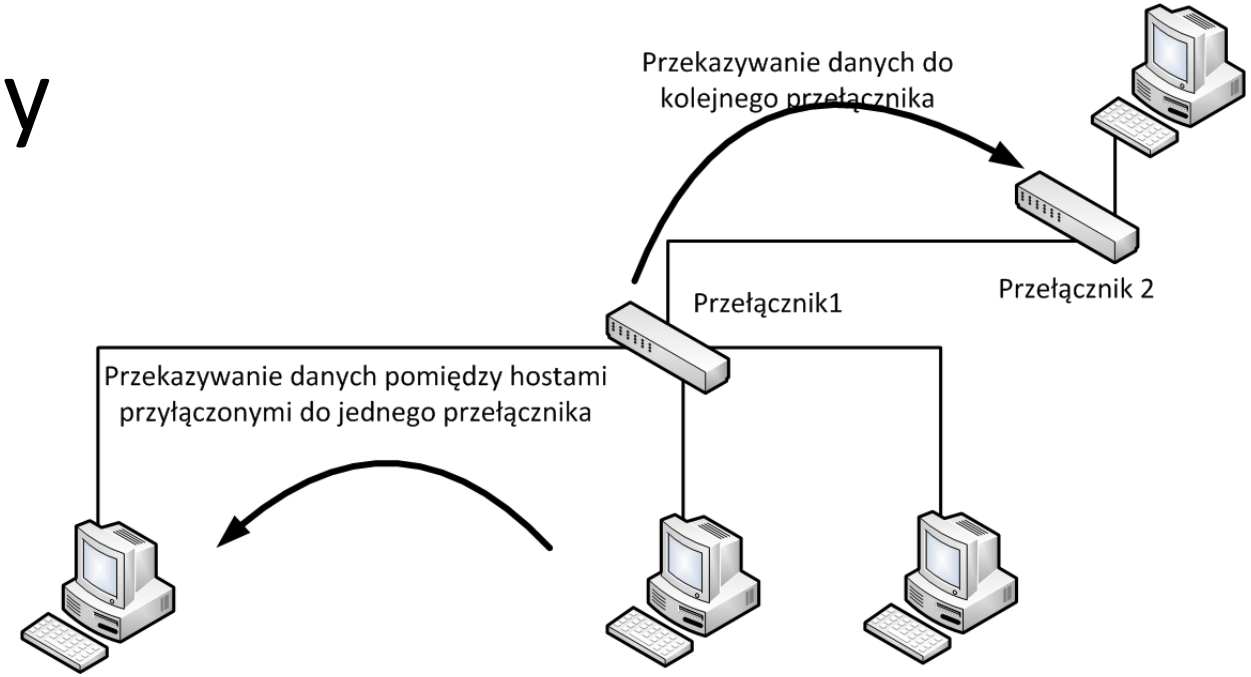
- Podstawowymi technikami klasycznego Ethernet są metoda nasłuchu łącza (ang. carrier sense) oraz dostępu wielokrotnego (ang. multiple access) z detekcją kolizji (ang. collision detection) – **CSMA/CD**.
- W przypadku gdy komputer A zamierza wysłać ramkę danych do komputera B, ale okazuje się, że w danej chwili komputer C wysyła dane do komputera D, to komputer A odkłada transmisję. Dzieje się tak, ponieważ komputer zamierzający rozpocząć nadawanie **nasłuchuje łącze**.
- Jeśli komputer nasłuchujący (A) stwierdzi, że łącze jest wolne, to rozpoczyna nadawanie. Może się jednak zdarzyć, że inny komputer (np. B) również w tym samym czasie rozpocznie swoją transmisję. Ponieważ podczas wysyłania pakietów komputery nadal nasłuchują łącze, **wykryją one kolizję** i przerwą swoje nadawanie, a następnie każdy z nich po odczekaniu losowego czasu podejmie ponowną próbę dostępu do łącza.

Ramka Ethernet



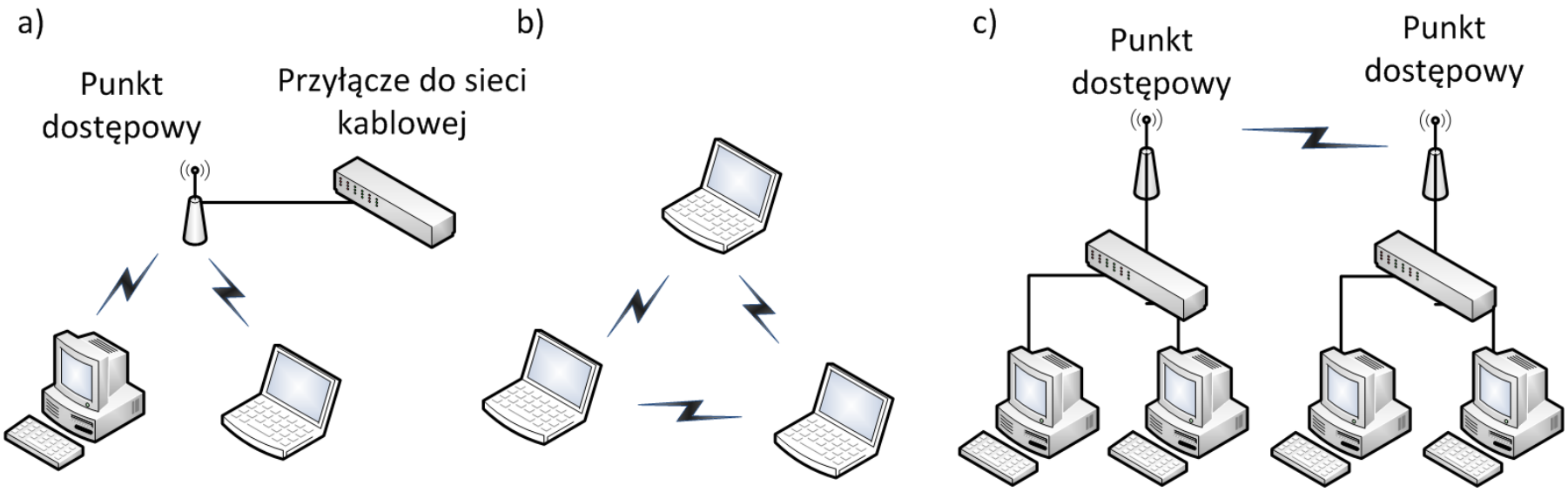
- Pierwsze dwa pola ramki o długości 6 bajtów każde zawierają odpowiednio jej adres docelowy i adres źródłowy. Każda karta sieciowa pracująca w standardzie Ethernet ma swój unikalny 48-bitowy (6-bajtowy) adres w skali całego świata (adres MAC). Dzięki temu przesłanie ramki danych pomiędzy dwoma urządzeniami w takim standardzie wymaga jedynie wskazania, kto dane chce przesłać i do kogo dane mają być wysłane.
- Dwubajtowe pole typu zawiera unikalną liczbę określającą rodzaj przesyłanych danych („stary” standard Ethernet) lub długość danych (standard 802.3).
- Kolejne pole ramki zawiera faktycznie przesyłane dane o długości od 48 do 1500 bajtów.
- Ostatnie czterobajtowe pole zawiera obliczoną z ramki tak zwaną sumę kontrolną (CRC - ang. Cyclic Redundancy Check). Jeśli po przesłaniu ramki i obliczeniu z niej sumy kontrolnej okazuje się, że wartość otrzymanej sumy jest inna niż wartość sumy przesłanej, to można stwierdzić, że dane uległy przekłamaniu.

Przełączany Ethernet

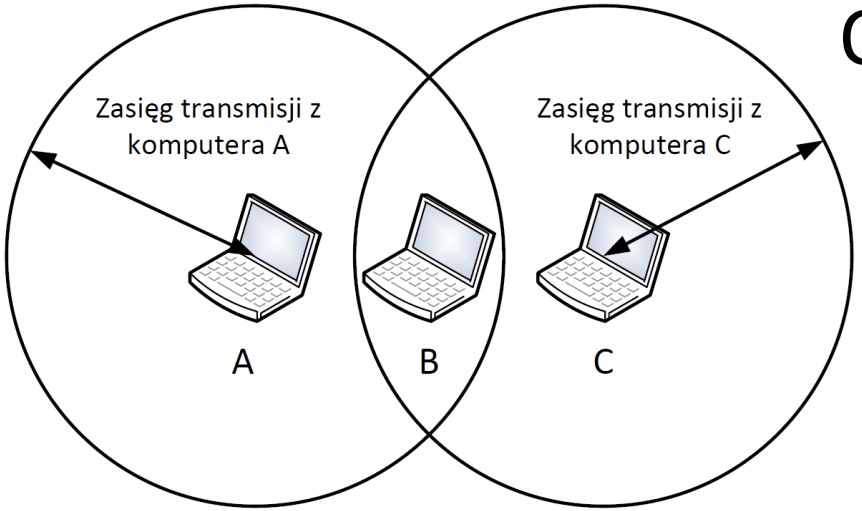


- Ethernet przełączany nie wykorzystuje metody CSMA/CD, ponieważ w strukturach sieci komputerowych opartych na przełącznikach nie następują kolizje.
- Ruchem ramek w sieci zarządzają **przełączniki**, które identyfikują nadawcę oraz odbiorcę i przesyłają strumień bitów przez odpowiedni kanał informacyjny. Przełączniki sprawdzają, do jakiego komputera mają być przesłane dane. Dysponują również skonfigurowaną przez użytkownika lub automatycznie wygenerowaną tablicą adresów Ethernet.
- W konsekwencji, jeśli nadawca i adresat są przyłączeni do tego samego przełącznika, to ruch w sieci ograniczany jest tylko do przekazywania ramek w jednym przełączniku.
- Jeśli przełącznik „stwierdzi”, że dane nie należą do żadnego z komputerów do niego przyłączonych, wyśle je do kolejnego przełącznika.

Konfiguracje sieci bezprzewodowych



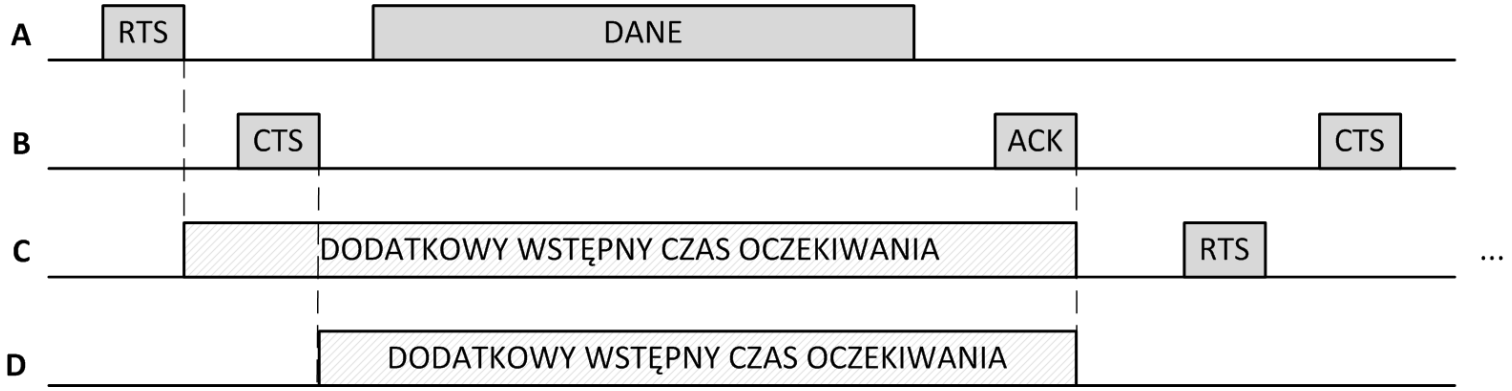
Ograniczona widoczność



W konstruowaniu sieci bezprzewodowych występuje wiele nowych problemów niespotykanych w przypadku sieci z trwałymi nośnikami informacji:

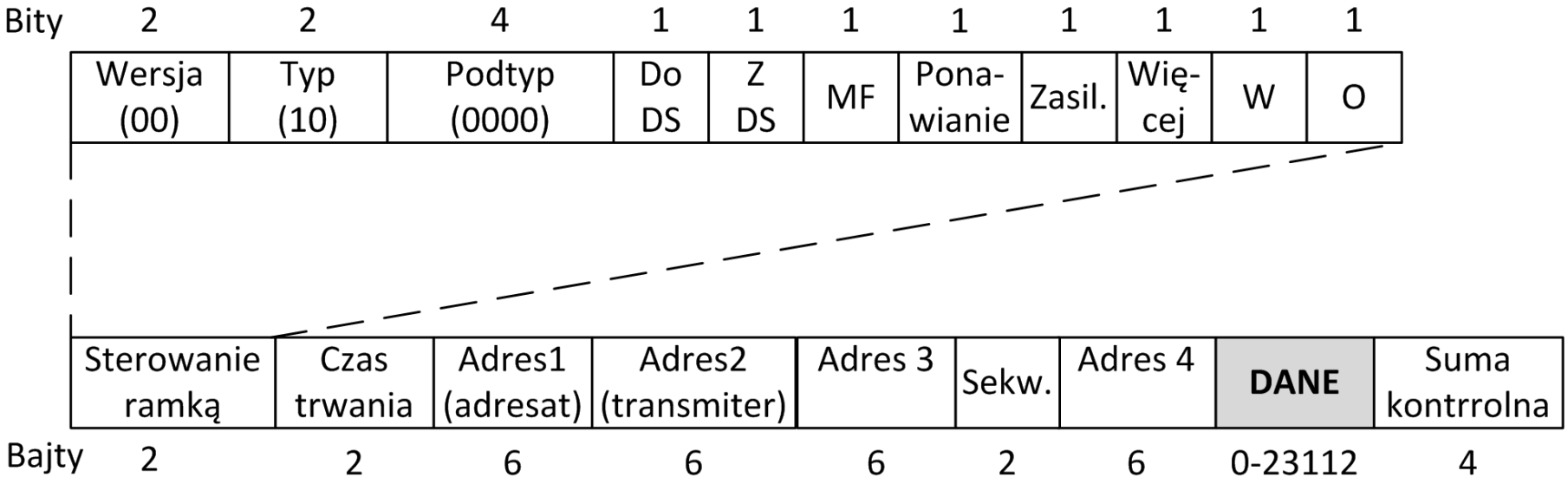
- wysoki współczynnik występowania błędów spowodowanych szumami elektromagnetycznymi występującymi w środowisku,
- realna szerokość pasma zależna od otoczenia i odległości między hostami, wzajemne zakłócanie się sieci w wyniku interferencji,
- niewielka moc transmisji ograniczona prawnie, co skutkuje również ograniczonym zasięgiem,
- niepełna wzajemna widoczność wszystkich uczestników ruchu w sieci (por. rys., np. jeśli stacja A „widzi” stację B i stacja B „widzi” stację C, to wcale nie oznacza, że stacja A „widzi” stację C, co może być źródłem kolizji),
- pakiety w sieciach radiowych są z założenia niezabezpieczone i rozgłaszane w eterze, wówczas należy mieć na uwadze problemy z osiągnięciem bezpieczeństwa i uwierzytelnienia tak transmitowanych danych.

Wymiana danych w sieciach bezprzewodowych



- Próba podjęcia przesyłu danych przez hosta rozpoczyna się od nasłuchiwania stanu łącza. Jeśli łącze jest wolne, zostaje wysłany pakiet, jeśli nie, to host czeka na zakończenie aktualnej transmisji, a następnie oczekuje jeszcze przez losowo wybrany przedział czasu.
- Usprawnienia:
  - Po odebraniu danych przez węzeł docelowy przesyła on pakiet potwierdzenia ACK (ang. ACKnowledgment). Jeśli nadawca nie otrzyma potwierdzenia, uznaje, że jego dane nie dotarły i ponawia ich transmisję;
  - Kiedy nadawca chce rozpocząć przekazywanie danych, wysyła do odbiorcy ramkę z prośbą o zezwolenie na wysyłanie – RTS. Jeśli odbiorca jest gotowy do odbioru danych, potwierdza to wysłaniem ramki CTS. Taka inicjalizacja transmisji wymiana¸ krótkich ramek informuje wszystkie hosty w zasięgu nadawcy i odbiorcy, że nastąpi między nimi komunikacja, co powoduje odroczenie wysyłania ramek przez innych nadawców. Dodatkowo wszystkie rodzaje ramek zawierają informację o długości danych, które będą przesyłane, co pozwala na ustalenie przez inne hosty wstępnego czasu oczekiwania zanim rozpoczną procedurę dostępu do łącza.

Ramka w sieci bezprzewodowej



Przesyłanie danych w formie bezprzewodowej na większe odległości

- Pierwszą barierą jest uzyskanie uniwersalnego pasma komunikacji na poziomie metropolii czy kraju, a więc pasma licencjonowanego. Pozwoli to na odpowiednie wzmocnienie sygnału i objęcie sieci większym obszarem.
  - Jednym ze standardów, który definiuje technikę transmisji bezprzewodowej w sieciach metropolitalnych, jest IEEE 802.16 (Wi-MAX, ang. Worldwide Interoperability for Microwave Access).
  - Warto również zwrócić uwagę, że obecnie są stosowane standardy pozwalające tworzyć bezprzewodowe sieci metropolitalne, a w przyszłości krajowe, czy globalne. Jednym z nich jest standard telefonii komórkowej czwartej generacji LTE (ang. Long Term Evolution), która jest nastawiona na transmisję danych, a połączenia głosowe są jedną z usług.

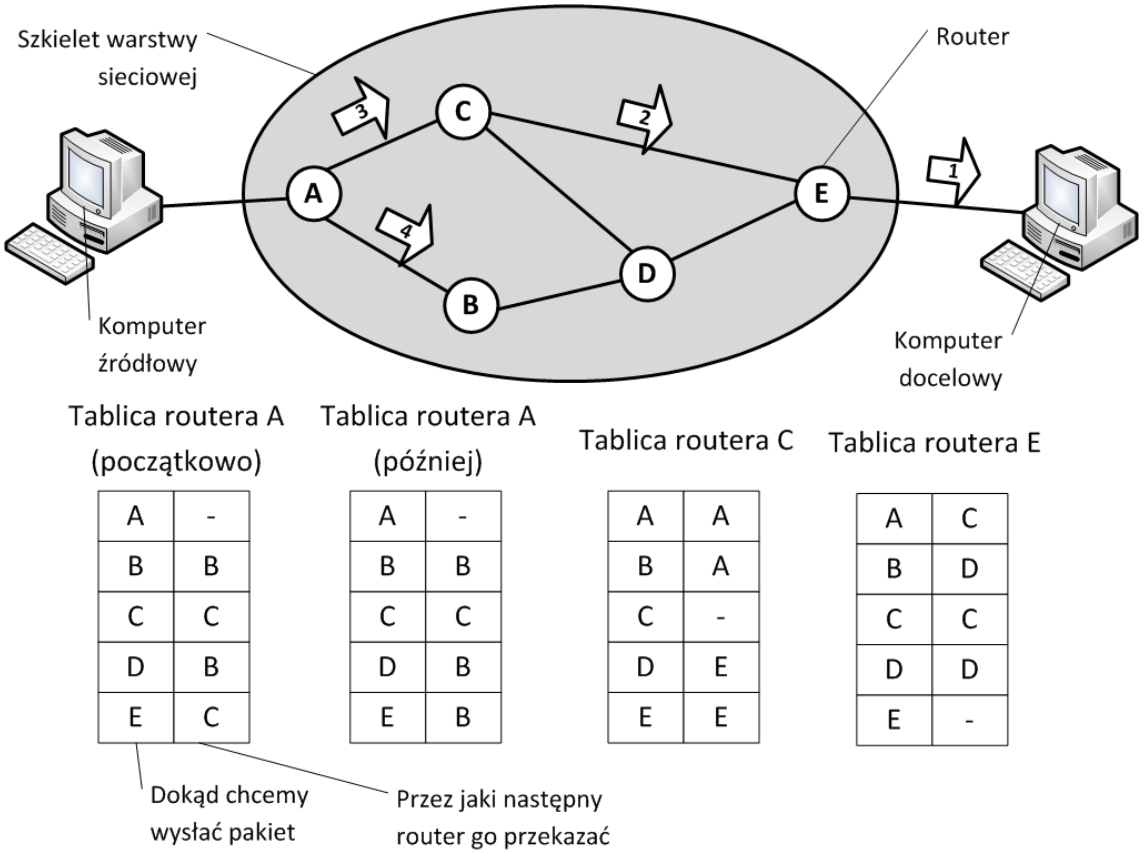
Standardy przesyłu danych w sieciach osobistych

- Równolegle z lokalnymi sieciami bezprzewodowymi skutecznie koegzystują technologie tworzenia bezprzewodowych sieci osobistych, a więc rozciągniętych na odległość do kilku metrów.
- Podstawowymi standardami przemysłowymi tworzenia takich systemów, które zostały uznane przez rynek, sa¸ Bluetooth i RFID (ang. Radio Frequency IDentification):
  - Standard Bluetooth umożliwia zbudowanie osobistej sieci komputerowej złożonej z bezprzewodowych urządzeń peryferyjnych komputera personalnego: klawiatury, myszy, drukarek czy aparatu fotograficznego.
  - Jest on również stosowany do komunikacji pomiędzy smartfonami a urządzeniami tak zwanej elektroniki ubieranej (np. zegarki, okulary, obuwie i ubrania wyposażone w odpowiednie moduły elektroniczne) oraz do włączania smartfonów w systemy komputerowe pojazdów samochodowych (systemy głośnomówiące itp.).
  - Standard RFID operuje na dwu typach urządzeń – znacznikach, które w niektórych wypadkach nie musza¸ być zasilane, oraz czytnikach, które z pewnej odległości są w stanie zinwentaryzować stan pobliskich znaczników.
  - Znaczniki maja¸ 96-bitowe identyfikatory oraz pewien niewielki obszar pamięci, którą można zapisać lub odczytać.
  - Okazuje się, że na podstawie miniaturowych znaczników, które mogą być wtapiane w dokumenty, wszczepiane zwierzętom, naklejane na paczki czy produkty handlowe, oraz odpowiednich czytników można skutecznie zorganizować m. in. bezprzewodowe systemy zarządzania przedsięwzięciami logistycznymi, zarządzania dostępem do pomieszczeń, ochrony własności, identyfikacji dokumentów, zwierząt i przedmiotów.

Warstwa sieciowa

- Gdyby standard Ethernet był jedynym obowiązującym na świecie, stworzenie globalnej sieci komputerowej nie stanowiłoby problemu. Unikalne adresy MAC urządzeń w skali całego świata znacznie by to ułatwiły. Jednak został on opracowany w czasie, gdy koncepcja i protokoły Internetu były na tyle dojrzałe, że nie dały się zepchnąć na margines. Ponadto do czasu wdrożenia techniki światłowodowej Ethernet oferował metodę komunikacji na niewielkie odległości.
- Istotą projektowania warstwy sieciowej stało się opracowanie mechanizmu do globalnej komunikacji komputerów, przy założeniu że są one połączone za pomocą różnych standardów komunikacyjnych, nazywanych w modelu odniesienia TCP/IP warstwą łącza danych (por. podrozdz. 1.3.3).
- Przełomem było zaproponowanie **systemu niescentralizowanego**. Do tamtej pory użytkownicy komputerów łączyli się na odległość z pojedynczymi komputerami, a nie z ich siecią. Opracowanie warstwy sieciowej zostało powiązane z wprowadzeniem na rynek nowych komputerów komunikacyjnych – **routerów**.
- Miały to być urządzenia, które po przesłaniu do nich odpowiedniego pakietu z danymi umiałyby go między sobą przekazywać, aż do „znalezienia” podsieci, w której znajduje się komputer docelowy – adresat pakietu.
- Kluczowym mechanizmem warstwy sieciowej stały się tak zwane **algorytmy routingu** – techniki generowania tabel wskazujących, do jakiego kolejnego routera ma zostać przekazany pakiet, aby osiągnął komputer docelowy.
- Istotnym składnikiem warstwy sieciowej było również opracowanie nowego **ogólnoświatowego mechanizmu adresacji komputerów** oraz formatu pakietów do przesyłania danych w takiej niejednorodnej sieci. Założono przy tym, że pakiety mogą być utracone oraz że mogą zostać pofragmentowane na mniejsze jednostki, jeśli dana podsieć nie będzie w stanie przesłać ich w całości.

Routing w sieciach rozległych



A	-
B	B
C	C
D	B
E	C

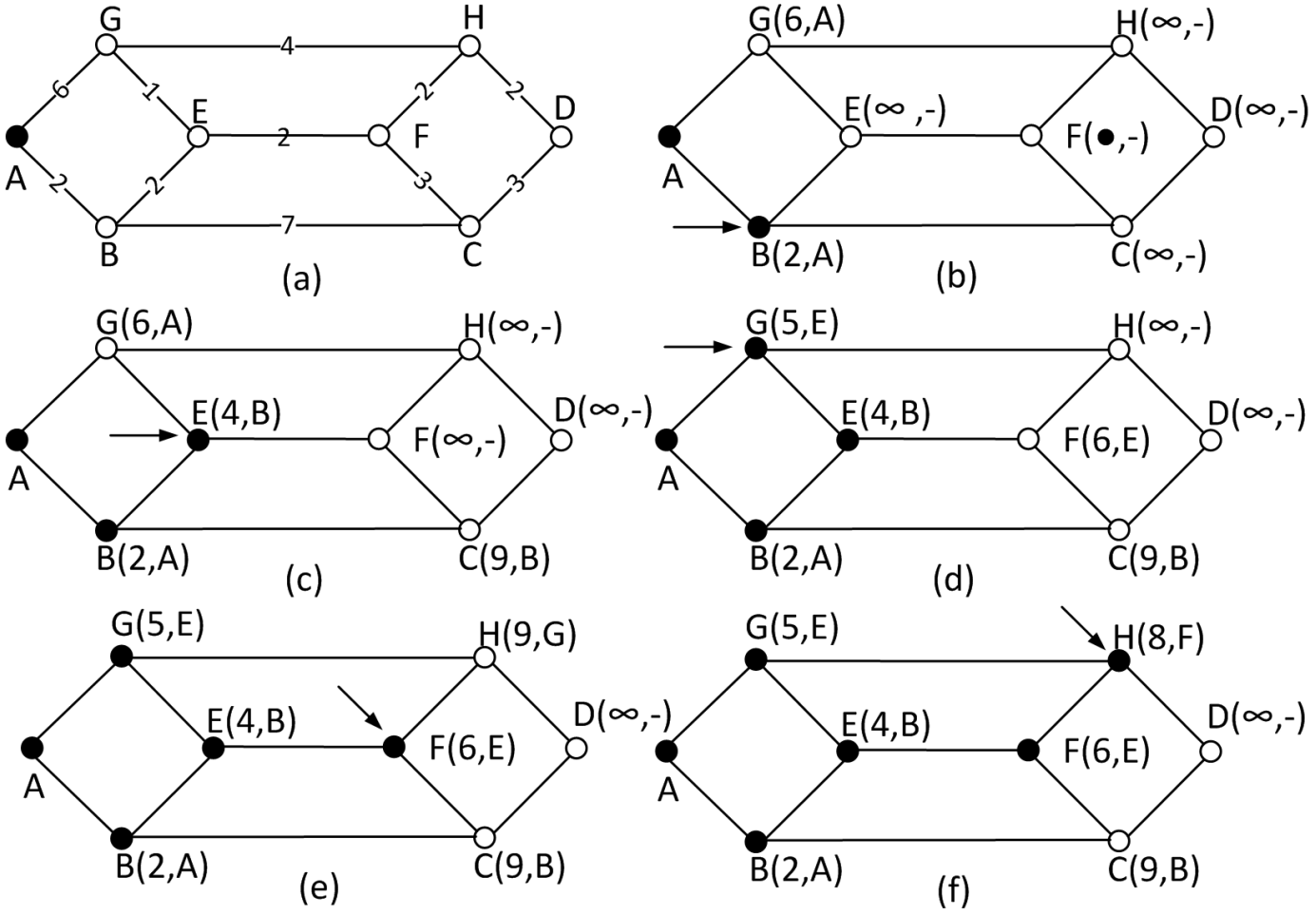
A	-
B	B
C	C
D	B
E	B

A	A
B	A
C	-
D	E
E	E

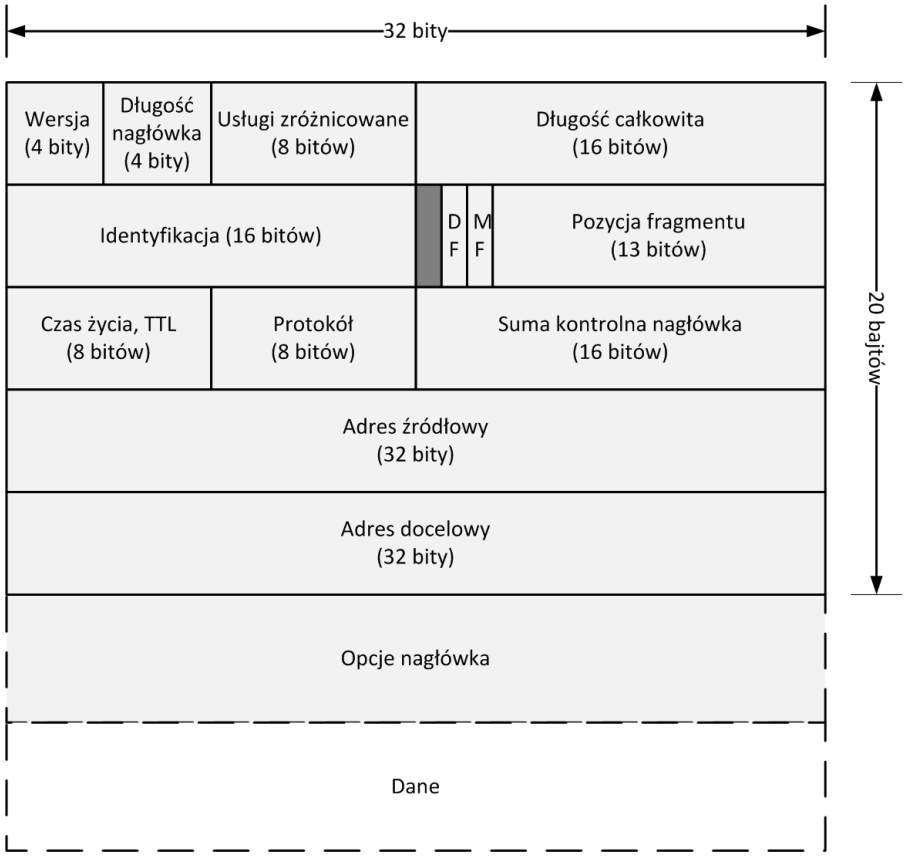
A	C
B	D
C	C
D	D
E	-

- Pakiety przesyłane w warstwie sieciowej posiadają jedynie adresy nadawcy i odbiorcy oraz „wskazówki” co do ważności przesyłanych danych. Nie zawierają jednak żadnych informacji, którędy miałyby być transportowane.
- Routery – podstawowe urządzenia komunikacyjne w warstwie sieciowej – „potrafią” na podstawie tych skąpych informacji wskazać trasę dla pakietów.
- Dodatkowo strumień danych podzielony na pakiety moše w warstwie sieciowej wędrować różnymi trasami, jeśli routery uznają to za „korzystne”.

Algorytm Dijkstry



IPv4



Wersja wskazuje, do jakiej wersji protokołu należy pakiet.

Długść nagłówka wskazuje, jak długi jest nagłówek pakietu w 32-bitowych słowach.

Usługi zróżnicowane : Pierwsze 6 bitów pola wskazuje klasę obsługi. Dwa ostatnie bity niosą jawną informacje, czy pakiet nie doznał przeciążenia.

Długość całkowita zawiera informacje o liczbie bajtów całego pakietu

Identyfikacja zawiera unikalną liczbę całkowitą wskazującą bieżący pakiet.

DF – pakiet nie może być fragmentowany

MF – bit oznaczający, że po tym pakiecie będzie przesyłany następny fragment.

Pozycja fragmentu wskazuje, jaki odcinek informacji z pola danych jest
przesyłany w danym fragmencie.

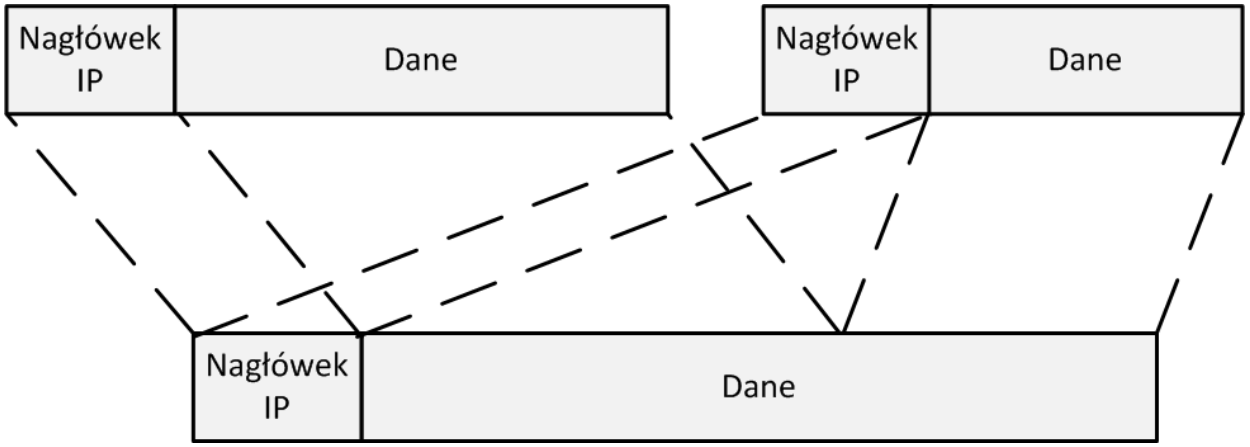
Czas życia przez ile routerów może jeszcze przeskoczyć pakiet

Protokół wskazuje proces transportowy, do którego w komputerze ma
być dostarczony pakiet.

Suma kontrolna nagłówka zawiera sumę kontrolną obliczoną z nagłówka,

Adres źródłowy i **adres docelowy** zawierają odpowiednio adres IPv4 nadawcy i odbiorcy pakietu.

Fragmentacja

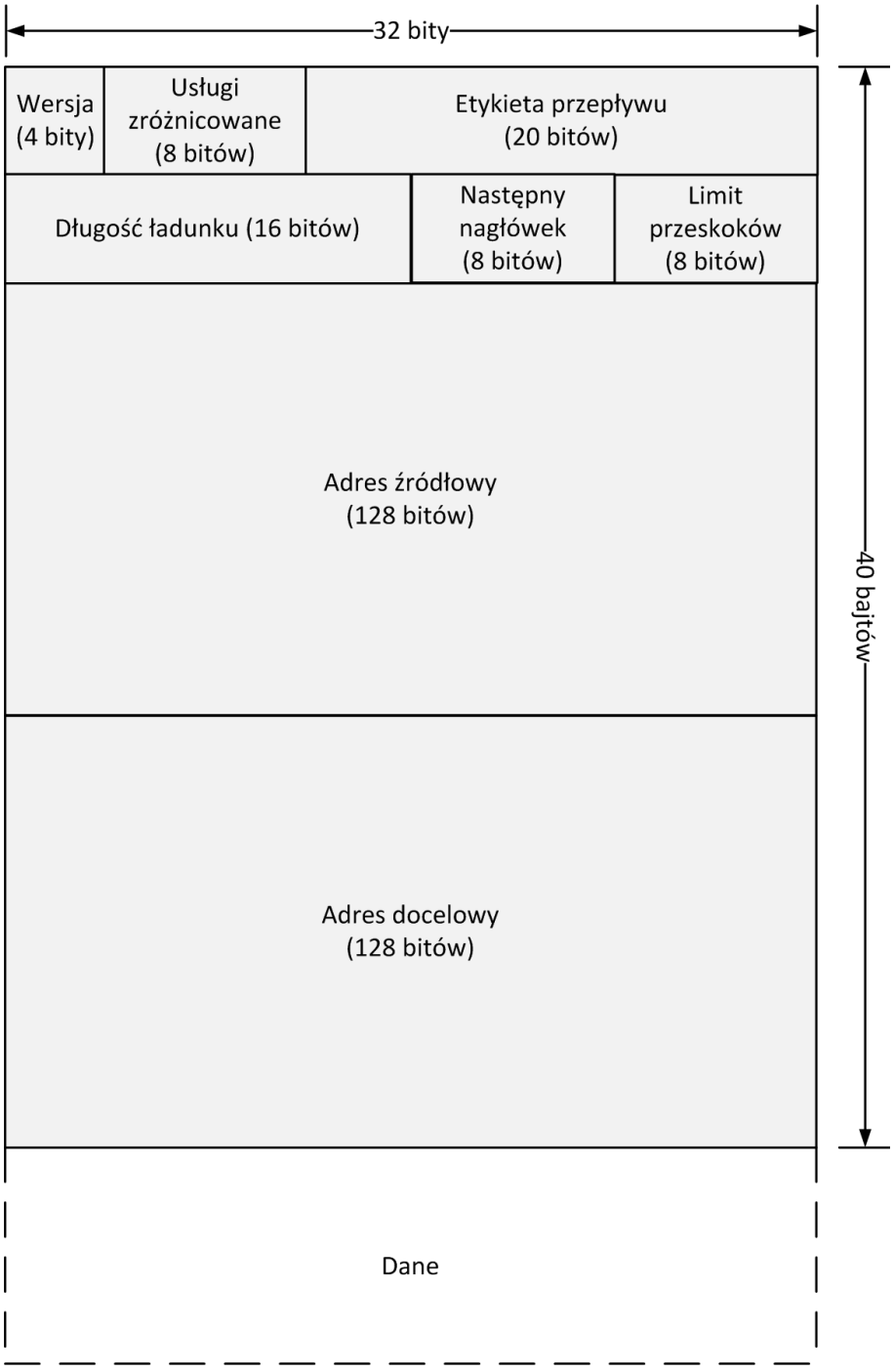


- Pakiety w czasie ich transportu mogą być dzielone na mniejsze fragmenty.
- Wszystkie fragmenty danego pakietu są pakietami IP zawierającymi takie samo pole identyfikacji, co umożliwia ich ponowne scalenie.
- W sterowaniu przepływem fragmentów biorą również udział bity DF i MF nagłówka.

Bezklasowy Routing Międzydomenowy

Listing 1.1

```
1  Adres IP:                        218.64.116.75
2  Maska sieci:                     255.255.255.192
3  Adres IP (binarnie):             11011010.01000000.01110100.01001011
4  Maska (binarinie):               11111111.11111111.11111111.11000000
5  Adres sieci (binarnie):          11011010.01000000.01110100.01000000
6  Adres sieci:                     218.64.116.64
7  Adres rozgoszeniowy
8   (binarnie):                     11011010.01000000.01110100.01111111
9  Adres rozgoszeniowy:             218.64.116.127
10 Adres pierwszego komputera
11 w sieci (binarnie):              11011010.01000000.01110100.01000001
12 Adres pierwszego komputera
13 w sieci:                         218.64.116.65
14 Adres ostatniego komputera
15 w sieci (binarnie):              11011010.01000000.01110100.01111110
16 Adres ostatniego komputera
17 w sieci:                         218.64.116.126
18 Dopuszczlna liczba
19 komputerow w podsieci:            61 (63-2)
```



IPv6

- Na jednym metrze kwadratowym Ziemi może się znajdować 7 x 10^{23} osobno zaadresowanych komputerów
- **Wersja**: 6
- **Usługi zróżnicowane**: jak w IPv4
- **Etykieta przepływu**: połączenie pakietów od jednego nadawcy do odbiorcy
- **Długość ładunku**: zawiera liczbę bajtów, które w danym pakiecie umieszczono po 40-bajtowym nagłówku.
- **Następny nagłówek** wskazuje, który z dostępnych sześciu opcjonalnych nagłówków znajduje się po pierwszym nagłówku pakietu.
- **Limit przeskoków: jak TTL IPv4**
- Adres nadawcy i adres odbiorcy (128bit)
- Notacja:

8020:0000:0000:0000:0124:4556:8945:CDDA

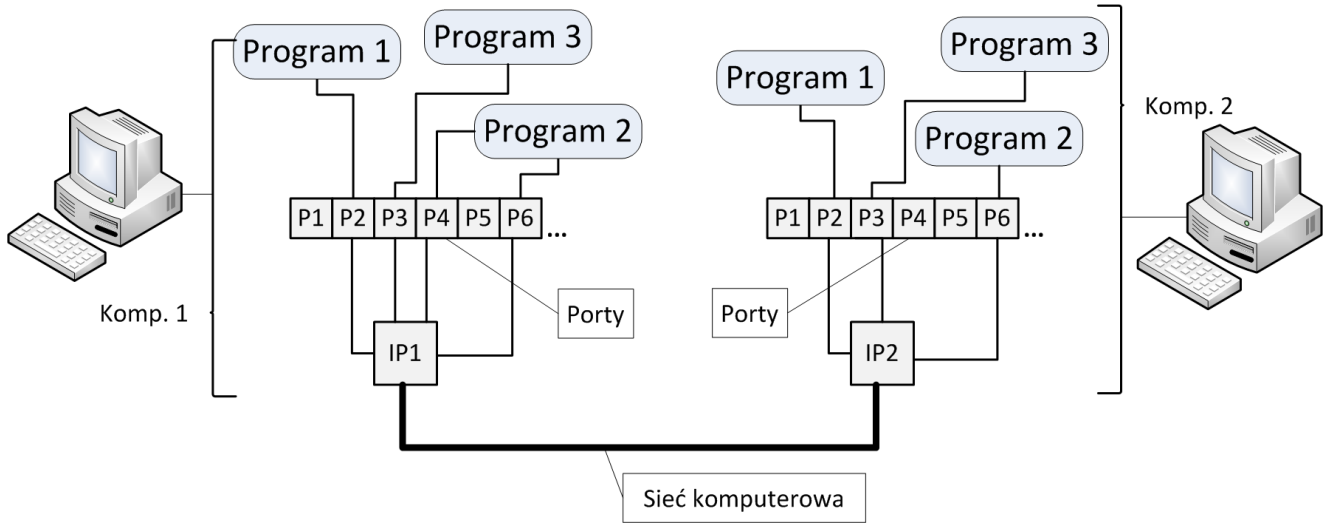
8020::124:4556:8945:CDDA

::192.31.17.22

Dodatkowe protokoły (warstwa sieciowa)

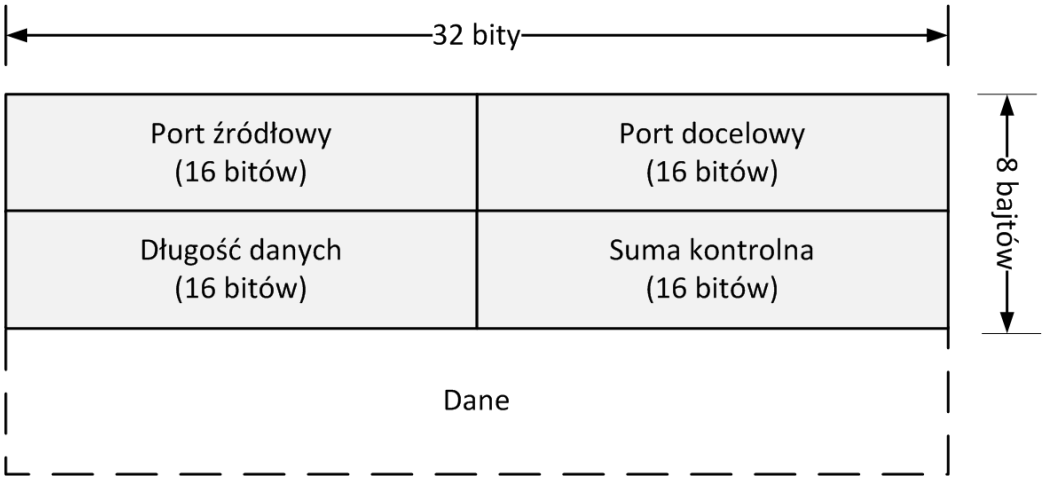
- ICMP (ang. Internet Control Message Protocol)
  - Komunikaty ICMP sa¸ przesyłane w ramkach IP. Najważniejszymi błędami zgłaszanymi w komunikatach ICMP są niemożliwość dostarczenia pakietów, zniszczenie pakietu z powodu osiągniącia przez pole czas życia/limit przeskoków wartości 0 czy błąd w polu nagłówka wskazujący na potencjalny błąd oprogramowania IP nadawcy lub jednego z routerów.
- ARP (ang. Address Resolution Protocol)
  - Protokół ARP służy do wiązania adresów IP z fizycznymi adresami (np. Ethernet) urządzen´ sieciowych. Zanim nastąpi przesyłanie danych zgodnych z protokołem IP do sieci są wysyłane rozgłoszeniowe pakiety formatu ARP z zapytaniem, który z komputerów posiada dany adres IP. Po otrzymaniu odpowiedzi nadawca wie, do którego fizycznego urządzenia należy przesłać pakiet opakowany w ramką. Komputer włączony w strukturą nowej sieci samodzielnie buduje mapę pomiędzy adresami IP i np. Ethernet.
- DHCP (ang. Dynamic Host Configuration Protocol).
  - Protokół DHCP „zwalnia” użytkownika z konieczności samodzielnego konfigurowania protokołu IP na swoim komputerze. Większość urządzeń podłączanych do sieci wymieniających pakiety zgodnych z protokołem IP jest tak skonfigurowana, że w chwili przyłączenia sią do nowej sieci poszukuje w niej komputera z uruchomionym serwerem DHCP. Serwer, posługując się mechanizmami warstwy łącza danych, przekazuje nowemu klientowi adres IP z zarezerwowanej puli. Wdrożenie protokołu DHCP uprościło łączenie sią z siecią zgodną z protokołem IP. Protokół pozwala równieą na racjonalne przydzielanie puli adresów, jeśli w podsieci znajduje się więcej komputerów nią dostępnych adresów

Porty



- Aplikacje, które chcą wysłać jakieś dane do sieci, wysyłają swoje strumienie danych przez dodatkowe „bramki” nazywane **portami**.
- Interfejs sieciowy przekształca te strumienie w łańcuchy pakietów IP przesyłanych przez sieć komputerową.
- Aplikacje, które chcą odbierać dane, „nasłuchują” na umówionych portach. Jeśli najdą się tam jakieś pakiety, to je odbierają, ponieważ uznają że są „zaadresowane” do nich.
- **Porty są dwustronnym medium komunikacji** i umożliwiają zarówno wysyłanie, jak i odbiór danych.
- **Zestawienie port i adres IP nosi nazwę gniazda** (ang. socket). Interfejs gniazd jest jednym z podstawowych zbiorów funkcji programistycznych do tworzenia aplikacji sieciowych.
- Numery portów od 0 do 1024 są tak zwanymi zarezerwowanymi numerami portów. W tym zakresie portów są już wyznaczone numery, na których podejmują komunikację powszechnie znane usługi sieciowe, takie jak WWW, FTP, IMAP. Przykładowo, wszystkie zapytania, które wysyła się do serwera WWW, są z założenia przekazywane na port 80.

Pakiet UDP

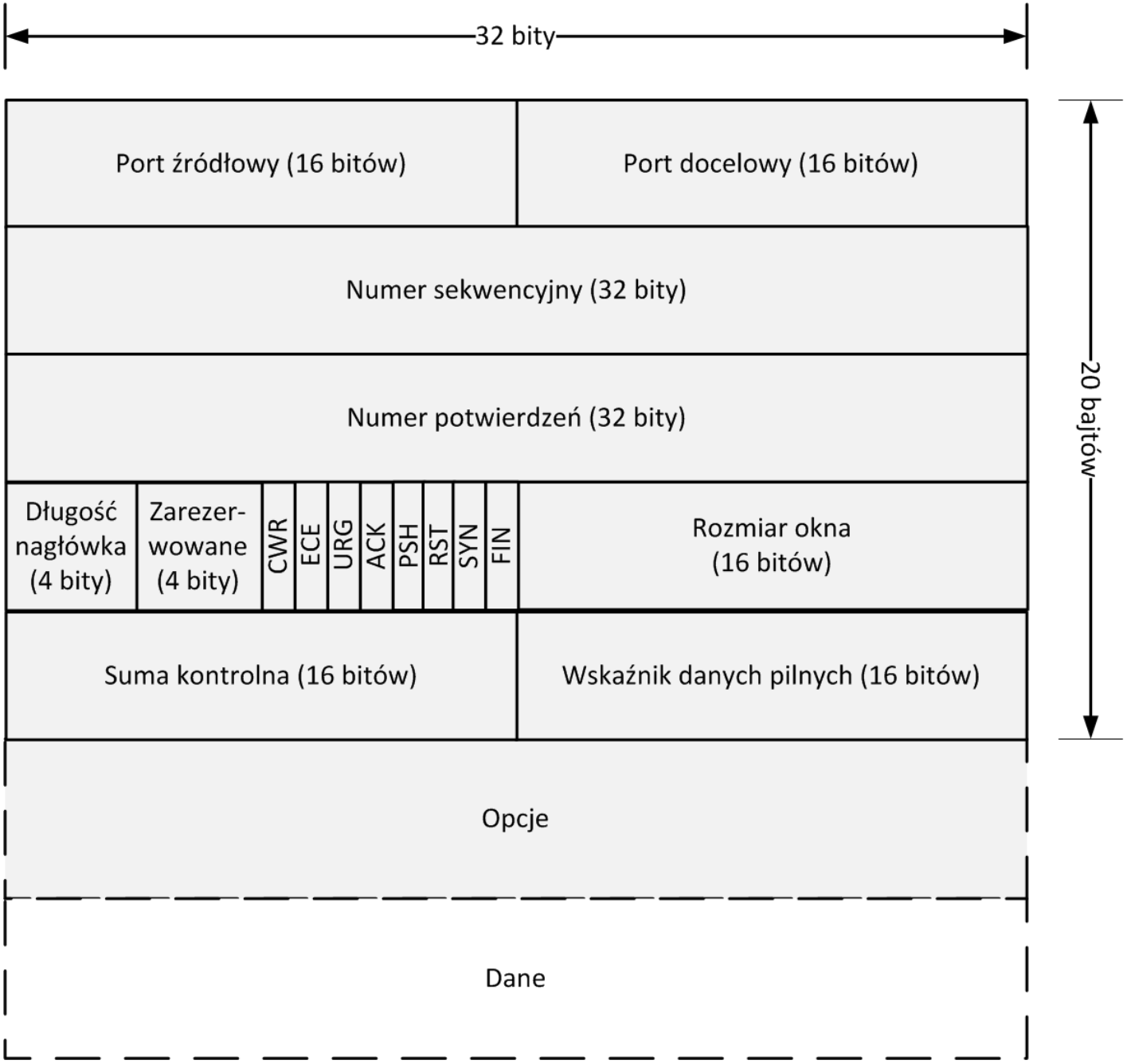


- Protokół UDP można uznać za swego rodzaju prostą „nakładkę” na protokół IP, umożliwiającą zestawienie łącza pomiędzy komputerami w warstwie transportowej.
- Protokół jest bezpołączeniowy i zawodny, to znaczy nie sprawdza, czy w sieci jest odbiorca gotowy na przyjmowanie danych oraz nie posiada wbudowanych mechanizmów sprawdzania, czy dany pakiet został dostarczony.
- Zastosowania: przesyłanie strumieni audio i wideo, komunikacja w grach sieciowych, dostarczanie informacji o nazwach domen (DNS - ang. Domain Name System), a nawet komunikacja w lokalnych sieciach komputerowych projektowanych na potrzeby przemysłu lotniczego.
- Nagłówek protokołu:
  - Numer portu źródłowego i numer portu docelowego.
  - Długość danych podaje długość pakietu UDP wraz z 8-bajtowym nagłówkiem.
  - Dla aplikacji wymagających większej niezawodności w nagłówku UDP można zamieścić sumę kontrolną.

Protokół TCP - charakterystyka

- Protokół TCP powstał w celu niezawodnego przesyłania danych na poziomie warstwy transportowej.
- Głównym mechanizmem zapewniającym niezawodność w przesyłaniu danych zgodnie z protokołem TCP jest potwierdzanie odebranych porcji danych w postaci specjalnych pakietów ACK (ang. ACKnowledgements) odsyłanych do nadawcy.
- Jeśli komputer A wysyła dane do komputera B, to komputer B musi wysłać do komputera A potwierdzenie o ich otrzymaniu.
- Jeśli potwierdzenie nie nadchodzi w założonym przedziale czasowym, następuje retransmisja tej samej porcji danych.
- W ramach protokołu TCP automatycznie są obliczane:
  - czas, jaki trzeba odczekać na odebranie potwierdzenia,
  - limit liczby ponownych potwierdzeń,
  - maksymalne opóźnienia po stronie odbiorcy na odesłanie potwierdzenia.
- Podczas przesyłania danych następuje również:
  - rozpoznawanie potwierdzeń dla pakietów dochodzących w przypadkowej kolejności,
  - porządkowanie danych przychodzących w przypadkowej kolejności,
  - rozpoznawanie powielonych pakietów,
  - regulacja szybkości przesyłanych pakietów.

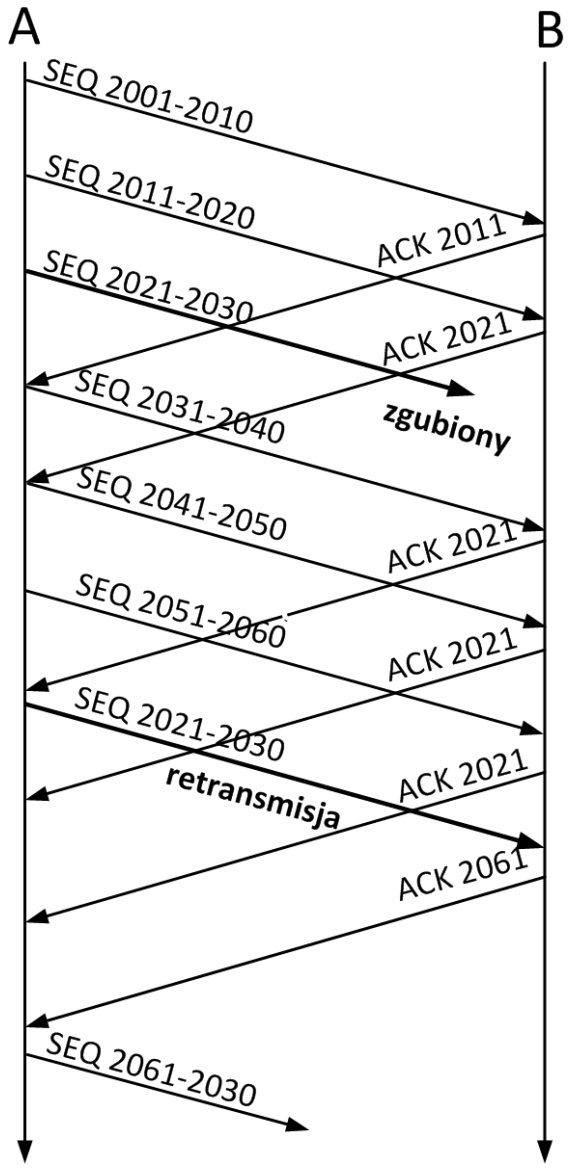
TCP


32 bity
Port źródłowy (16 bitów)
Port docelowy (16 bitów)
Numer sekwencyjny (32 bity)
Numer potwierdzeń (32 bity)
Długość nagłówka (4 bity)
Zarezer-wowane (4 bity)
CWR
ECE
URG
ACK
PSH
RST
SYN
FIN
Rozmiar okna (16 bitów)
Suma kontrolna (16 bitów)
Wskaźnik danych pilnych (16 bitów)
Opcje
Dane
20 bajtów

Znaczenie pól nagłówka TCP

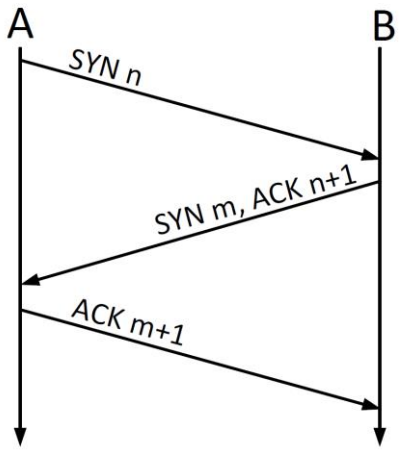
- Numer portu źródłowego i numer portu docelowego – ustalenie punktów połączenia strumienia danych z aplikacjami
- Numer sekwencyjny – losowa liczba zwiększana o 1 (mod 32) z przesłaniem każdego kolejnego bajta danych
- Numer potwierdzenia – wypełniane w datagramach potwierdzeń, zawiera informację o numerze bajta, na który teraz oczekuje odbiorca
- Długość nagłówka – liczba 32-bitowych słów, z których składa się nagłówek
- 4 zarezerwowane bity – dotąd nie mające zastosowania
- 6 bitów zawiera znaczniki (flagi) pozwalające na dodatkową identyfikację przesyłanego pakietu TCP, między innymi:
  - ECE, CWR – sygnalizacja przeciążeń
  - URG – w strumieniu są przesyłane pilne dane, do bajta wskazanego w polu „wskaźniki pilnych danych”
  - ACK – ustawiony = to jest pakiet potwierdzenia
  - PSH – dane powinny być natychmiast wysłane
  - RST – nadawca żąda resetu połączenia
  - SYN/FIN – stosowane w procedurze nawiązywania połączenia
- Rozmiar okna – ustawia odbiorca = ile bajtów nadawca może jeszcze przesłać od nr potwierdzenia; jeśli 0, to transmisja ma być wstrzymana
- Suma kontrolna jest liczona z nagłówka + pseudonagłówka
- Wskaźnik pilnych danych – pierwszy bajt, który nie jest już pilny.

TCP – potwierdzenia



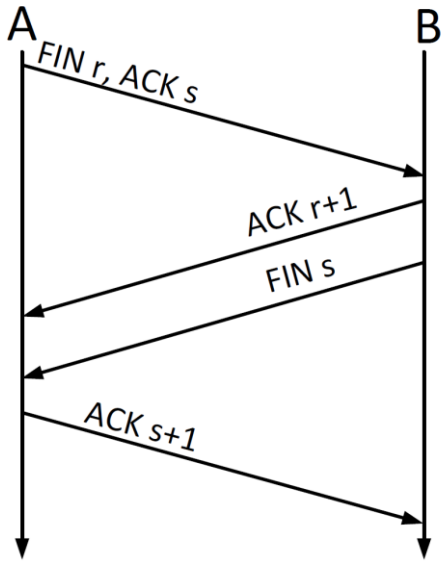
- Komputer A przesyła dane do komputera B zgodnie z protokołem TCP w porcjach po 10 bajtów.
- Segmenty zawierające dane bajty o numerach 2001-2010 oraz 2011-2020 zostały przesłane poprawnie i ich otrzymanie przez komputer B zostało potwierdzone odpowiednimi pakietami ACK.
- Niestety pakiet zawierający bajty 2021-2030 nie został dostarczony komputerowi B. Kiedy komputer B otrzymuje kolejny pakiet, odsyła pakiet potwierdzenia z numerem 2021, informując komputer A, że wciąż oczekuje na pakiet zawierający bajty o numerze od 2021.
- Dzieje się tak za każdym razem, gdy komputer otrzymuje inny pakiet niż ten rozpoczynający się od bajtu 2021.
- Po retransmisji sekwencji bajtów 2021-2030 komputer B potwierdza odebranie bajtów 2021-2060 w jednym pakiecie potwierdzenia.
- Pomimo wykrycia utraty pakietu 2021-2030 pakiety nadsyłane z komputera A były zapamiętywane i zostały po odzyskaniu straconego pakietu odpowiednio „ułożone” w strumieniu odbieranych danych.
- O skutecznym odzyskaniu strumienia danych informuje
- komputer B pakietem potwierdzenia o numerze 2061.

Nawiązywanie połączenia



- Komputer odbierający jest w stanie aktywnego oczekiwania.
- Inicjator połączenia ustala swój numer sekwencyjny i wysyła do komputera odbierającego pakiet zawierający ten numer wraz z ustawionym bitem SYN.
- Komputer odbierający odsyła wygenerowany przez siebie numer sekwencyjny wraz ze zwiększonym o jeden numerem sekwencyjnym inicjatora połączenia włączonym do pola numer potwierdzeń. Pakiet zawiera również ustawione bity SYN i ACK
- Z kolei komputer inicjujący odsyła do odbierającego pakiet potwierdzający (z ustawionym bitem ACK), zawierający powiększoną o jeden wartość pola numer sekwencyjny komputera odbierającego w polu numer potwierdzeń oraz ze zwiększoną o jeden wartością własnego pola numer sekwencyjny.

Zakończenie połączenia TCP



- Komputer inicjalizujący zamknięcie wysyła do komputera odbierającego pakiet potwierdzenia z ustawionym bitem FIN.
- Komputer odbierający odsyła pakiet potwierdzenia, a następnie sam wysyła pakiet sygnalizujący zakończenie połączenia (z ustawionym bitem FIN).
- Całkowite zamknięcie połączenia odbywa się po otrzymaniu przez komputer odbierający pakietu potwierdzenia od komputera inicjalizującego zamknięcie.

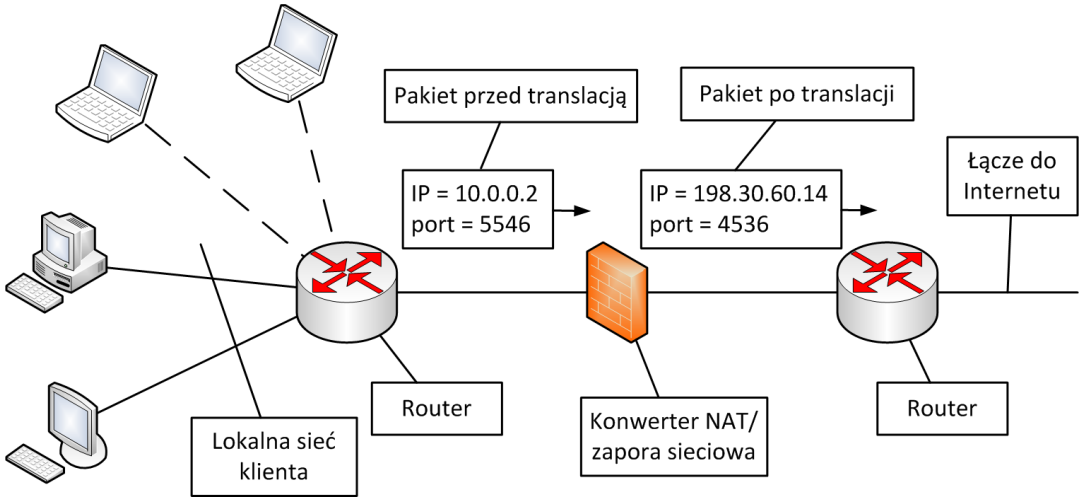
Sieci prywatne

Listing 1.2

```
1   10.  0.  0.  0   -    10.255.255.255/8  (16777216 adr. IP)
2  172. 16.  0.  0   -   172. 31.255.255/12 ( 1048576 adr. IP)
3  192.168.  0.  0   -   192.168.255.255/16 (   65536 adr. IP)
```

- **Adresy prywatne** nigdy nie zostaną przydzielone żadnemu komputerowi w publicznym Internecie. Pakiety o tych adresach mogą być wymieniane w obrębie sieci lokalnych (prywatnych) i nie są przepuszczane przez routery „na zewnątrz”.
- Oprócz adresów prywatnych w puli adresów Internetu istnieje jeszcze kilka zakresów adresów o specjalnym przeznaczeniu:
  - 0.0.0.0 jest rozumiany jako adres całego Internetu
  - 255.255.255.255 jest teoretycznie adresem rozgłoszeniowym do wszystkich komputerów w Internecie (z oczywistych względów takie rozgłoszenie odbywa się realnie tylko w danej podsieci, oddzielonej od Internetu routerem)
  - 127.0.0.1 – adres pętli - adres umożliwiający skonfigurowanie komunikacji poprzez interfejs sieciowy pomiędzy programami znajdującymi sią na jednym komputerze. Jest to zawsze adres komputera, na którym właśnie wykonujemy pracę.
  - 127.0.0.2 do 127.0.0.255 także należą do wewnętrznych adresów komputera.
  - Adresy mające pierwszy bajt z zakresu od 224 do 239 są zarezerwowane do prowadzenia tak zwanej komunikacji grupowej
  - Pierwszy bajt od adresu 239 – grupa adresów zarezerwowanych

NAT (ang. Network Address Translation)



- Pakiet z adresem klienta należącym do puli adresów prywatnych, który chce odwołać się do „zewnętrznego” adresu IP, jest w konwerterze NAT „przeadresowywany” (zmieniane jest pole adresu nadawcy).
- Po przejściu przez konwerter uzyskuje on inny adres pozwalający na swobodne przenoszenie pakietu w sieci nadrzędnej.
- Odpowiedź do klienta przychodząca z Internetu jest z kolei „przeadresowywana” przez konwerter z powrotem na jego adres w sieci lokalnej, co z kolei umożliwia efektywne odbieranie danych z Internetu.
- Zatem lokalna podsieć prywatna jest widoczna „na zewnątrz” konwertera NAT jako pojedynczy komputer z danym adresem IP.
- Technika NAT rozwiązała problem brakujących adresów IPv4. Instytucje, które chcą korzystać z zasobów Internetu, mogą „być widoczne” w postaci jednego komputera z pojedynczym adresem IP.

DNS (ang. Domain Name System)

Jedną z podstawowych usług warstwy aplikacji jest DNS (ang. Domain Name System). Serwery DNS dostarczają informacji o adresie IP posiadanym przez komputer identyfikowany za pomocą łańcucha tekstowego (np. www.rsa.com).
Na początku działania Internetu uzgodniono konwencję tworzenia nazw komputerów. Przyjęto podział nazw na tak zwane domeny, które z kolei dzielą się na poddomeny itd. Internet został podzielony na 250 domen najwyższego poziomu. Domeny najwyższego poziomu podzielone są na dwie kategorie: rodzajowe (np. gov, com) i narodowe (np. pl, uk).

Typowa konfiguracja komputera podłączonego do Internetu oprócz adresu IP, maski, adresu IP najbliższego routera (bramy) zawiera również wskazanie serwera DNS, który będzie dla danego komputera tłumaczył nazwy typu firma.com.pl na adres IP.

Domena	Planowane przeznaczenie	Data utworzenia
com	zastosowanie komercyjne	1985
edu	instytucje edukacyjne	1985
gov	instytucje rządowe	1985
int	organizacje międzynarodowe	1988
org	organizacje niekomercyjne	1985
aero	transport lotniczy	2001
mobi	urządzenia mobilne	2005

Protokoły warstwy aplikacji

- HTML – pobieranie plików sformatowanych z zastosowaniem odpowiedniego formatu
- SMTP (ang. Simple Mail Transfer Protocol) za pomocą odpowiednich komend umożliwiał połączenie się z serwerem przechowującym wiadomości, ich tworzenie, odczyt, usuwanie czy przesłanie do innego adresata.
  - Współczesne programy komunikujące się z serwerami poczty wciąż używają tego protokołu, tylko dla użytkowników jest on ukryty, a rezultaty jego „pracy” są widoczne w postaci graficznej na ekranie komputera.
  - Pierwotnie wiadomości pocztowe zawierały tylko tekst. Po wprowadzeniu zasad kodowania zgodnych z MIME (ang. Multipurpose Internet Mail Extension) wiadomości pocztowe mogły prze nosić dowolne rodzaje danych. Kodowanie MIME przekształca dowolne ciągi bajtów w taki sposób, że mogą być rozumiane jako znaki w kodowaniu ASCII.
- FTP (ang. File Transfer Protocol). Jest to protokół umożliwiający przesyłanie dowolnych plików pomiędzy komputerami. Ponownie odpowiednie komendy tekstowe umożliwiają przeglądanie katalogów plików na zdalnym komputerze oraz wysyłanie lub odbieranie plików do określonego katalogu. Użytkownicy współczesnych komputerów stosują ten protokół, kiedy kopiują pliki z Internetu na lokalny komputer lub kiedy wysyłają jakieś pliki poprzez odpowiednie formularze na stronach WWW.
- SFTP jest wersją protokołu zapewniającą szyfrowanie danych podczas przekazywania
- Telnet umożliwiał łącznie się do zdalnych konsol. Obecnie jest zastąpiony przez SSH, także pozwalające na łączenie ze zdalną konsolą, ale przez chronione łącze.
- Szereg programów jest rozwinięciem pomysłu SSH, ale pozwalają na korzystanie zdalne wprost z graficznego pulpitu zdalnego komputera.