

---

# Niższe warstwy

Sieci komputerowe

Wykład 5

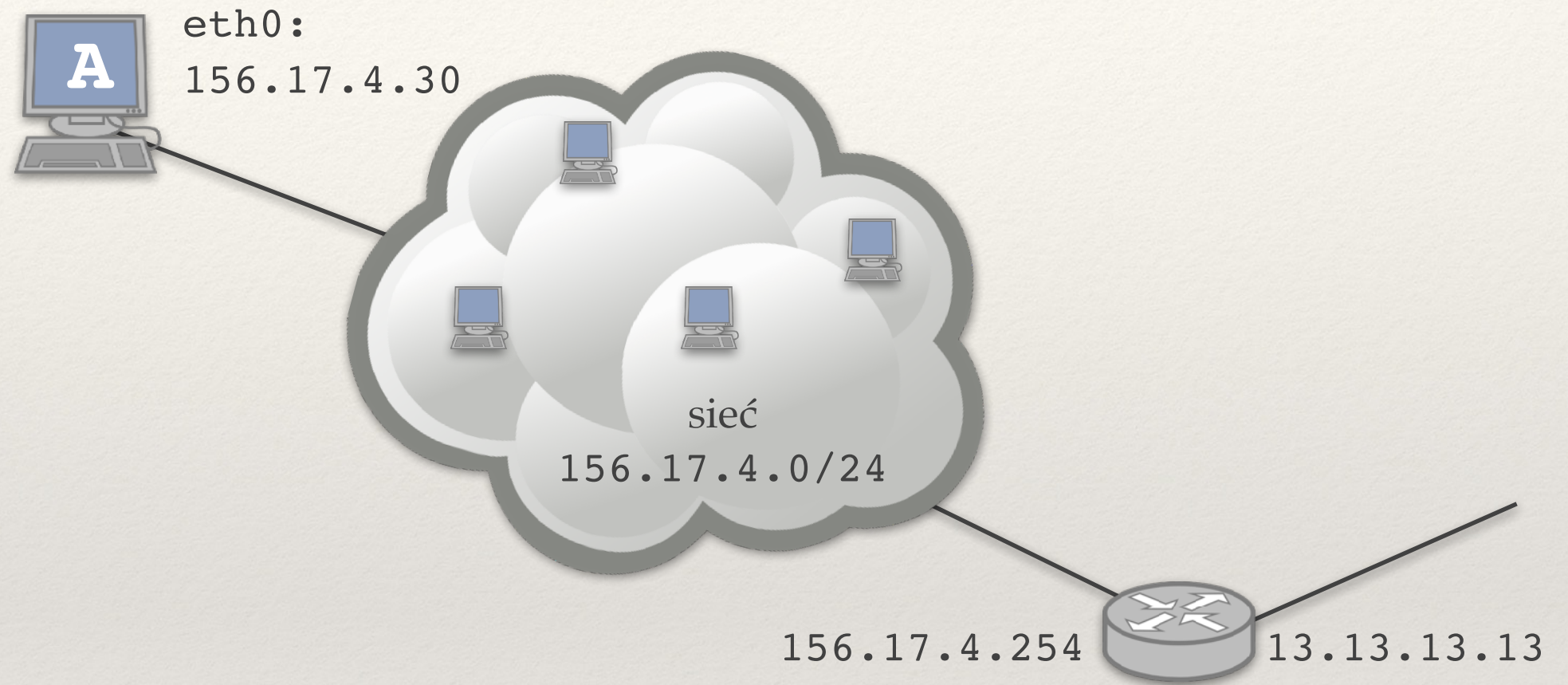
---

*Marcin Bieńkowski*



# Z punktu widzenia warstwy sieciowej

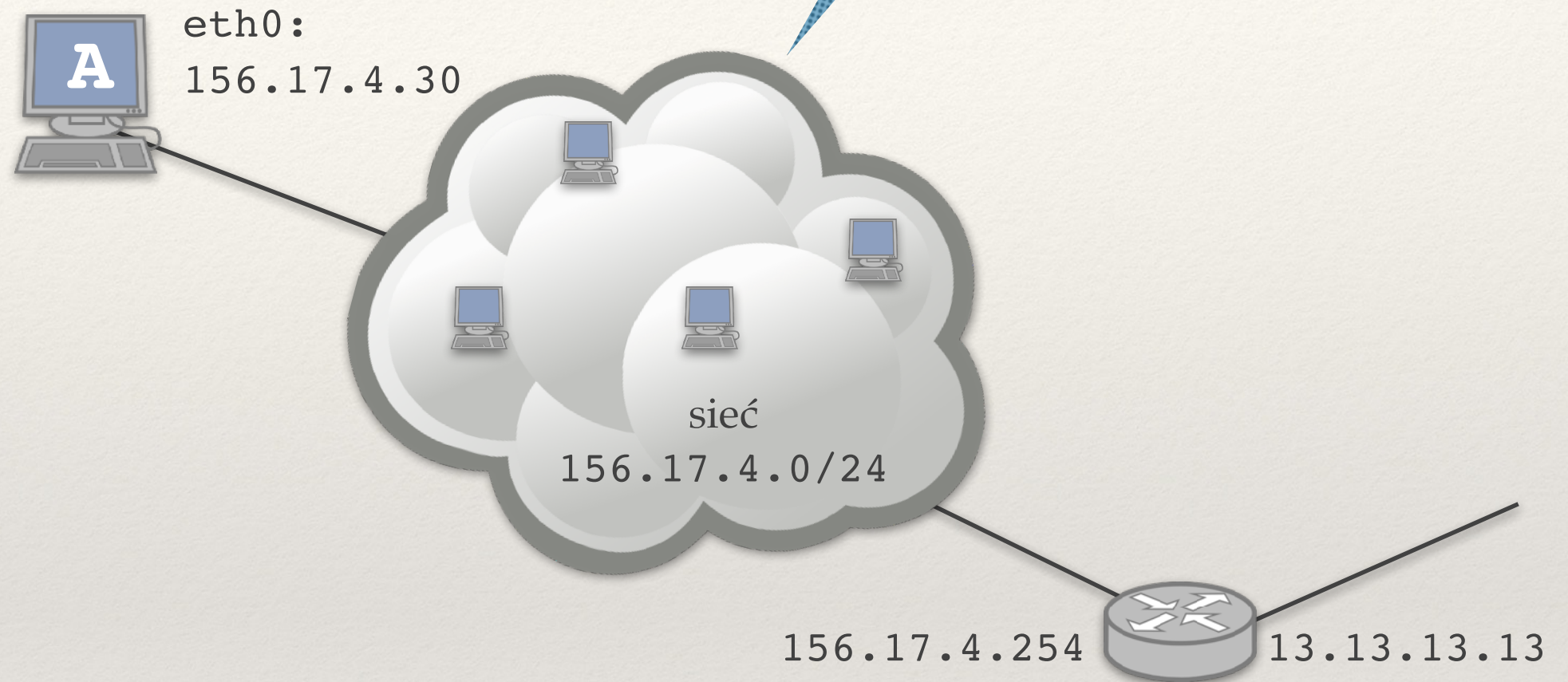
---





# Z punktu widzenia warstwy sieciowej

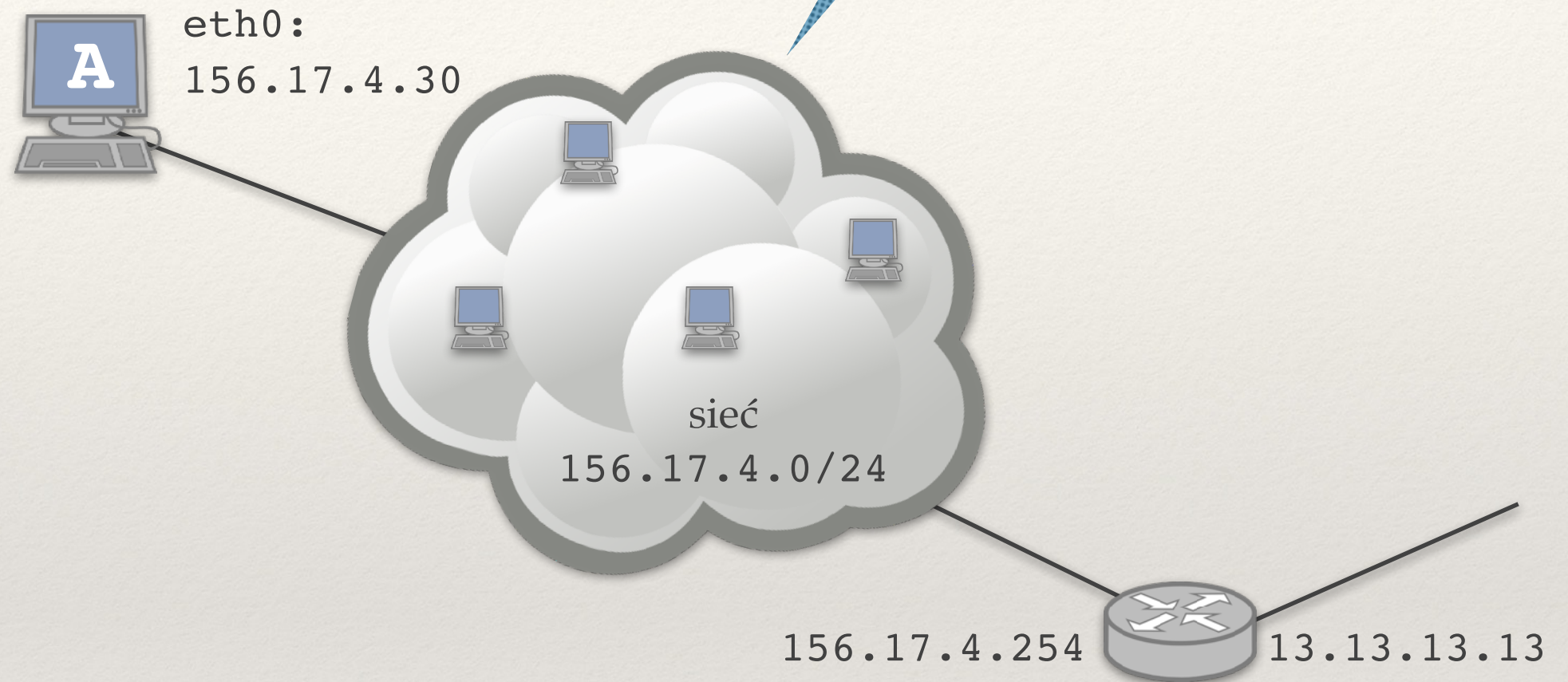
Co tu właściwie jest?





# Z punktu widzenia warstwy sieciowej

Co tu właściwie jest?

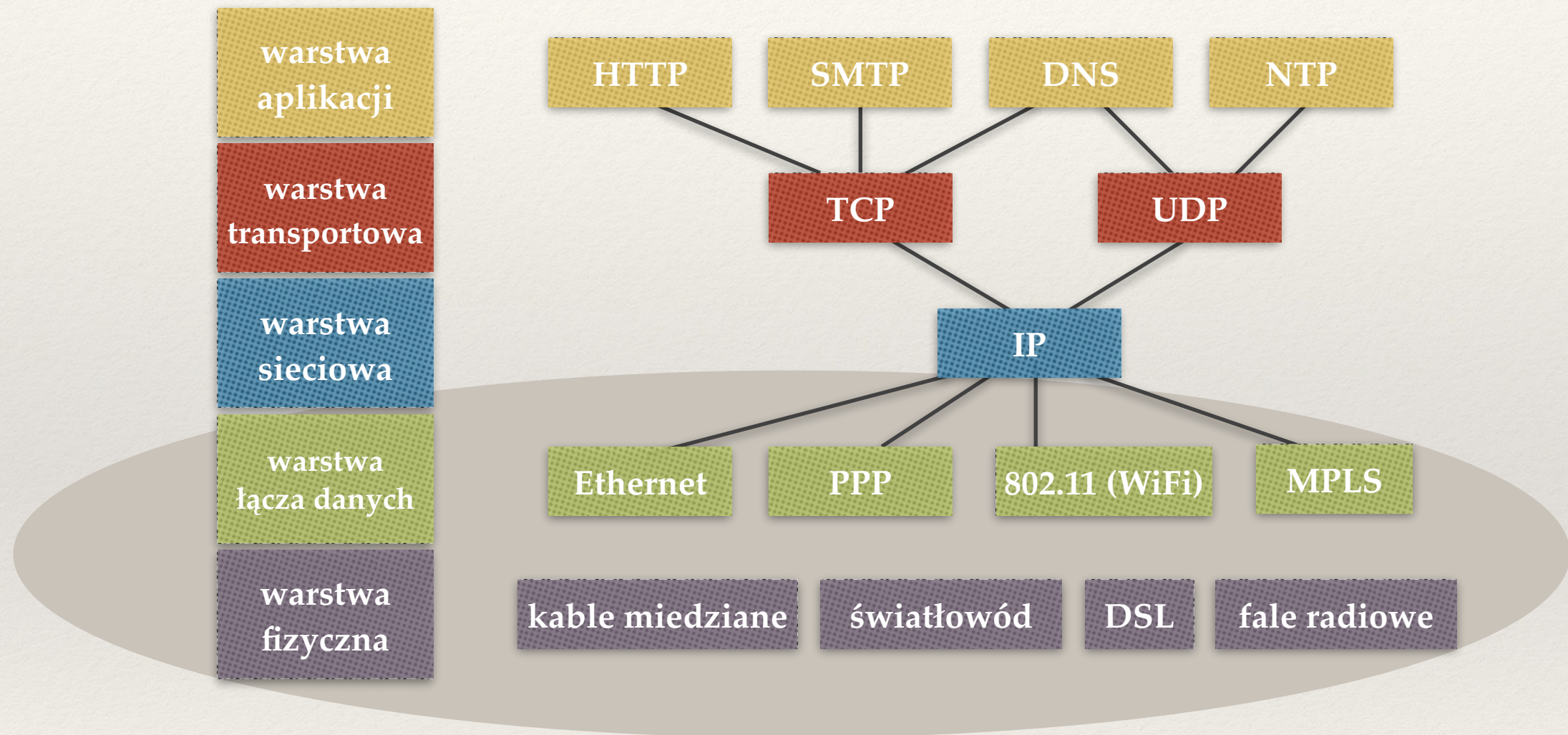


Co się dzieje, kiedy A wysyła pakiet do:

- 156.17.4.254?
- 156.17.4.255? (adres rozgłoszeniowy)



# Internetowy model warstwowy





# Dwie warstwy

---

## ❖ Warstwa łączy danych

- ♦ Umożliwia komunikację między dwoma „sąsiadującymi” urządzeniami.
- ♦ Zapewnia zawodną usługę wysyłania *ramek*.
- ♦ Kanał komunikacyjny może być współdzielony między wieloma urządzeniami.
- ♦ Musi radzić sobie z błędami transmisji.

## ❖ Warstwa fizyczna

- ♦ Określa szczegóły przesyłania pojedynczych bitów.

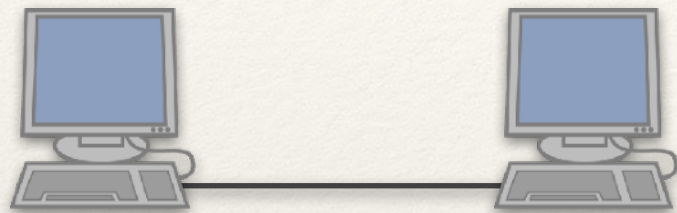
## ❖ Obie warstwy implementowane w kartach sieciowych

- ♦ Najczęściej implementacja sprzętowa.

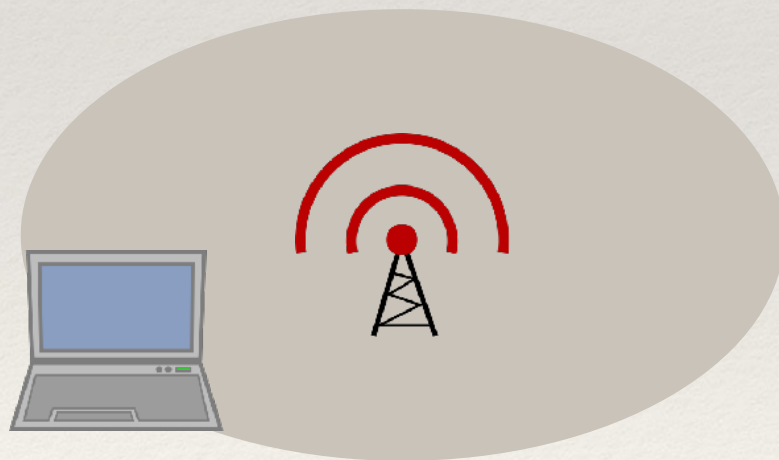


# Połączenia dwupunktowe

---



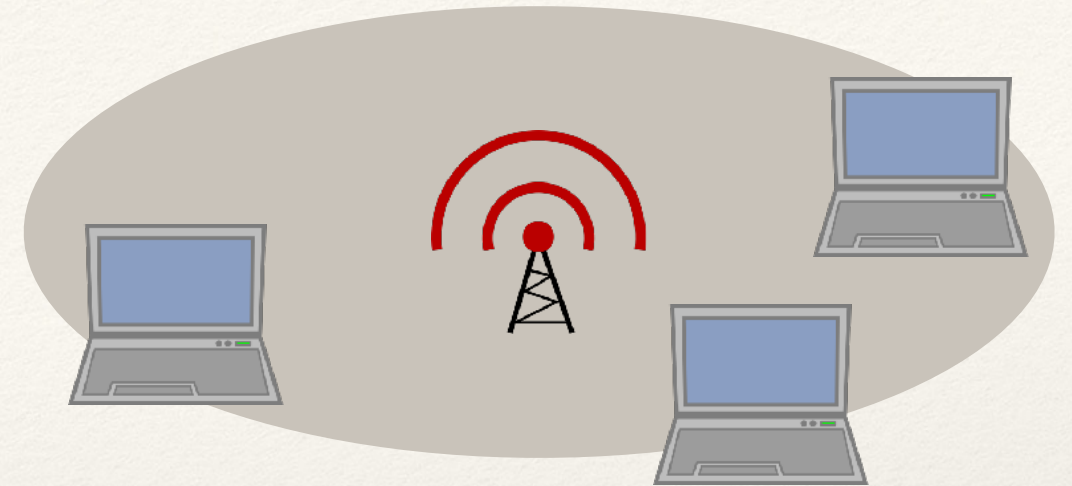
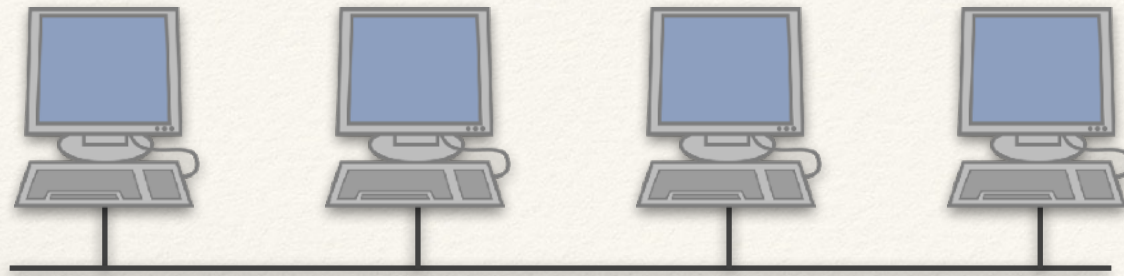
Komunikacja półdupleksowa lub pełnodupleksowa w zależności od możliwości kabla.



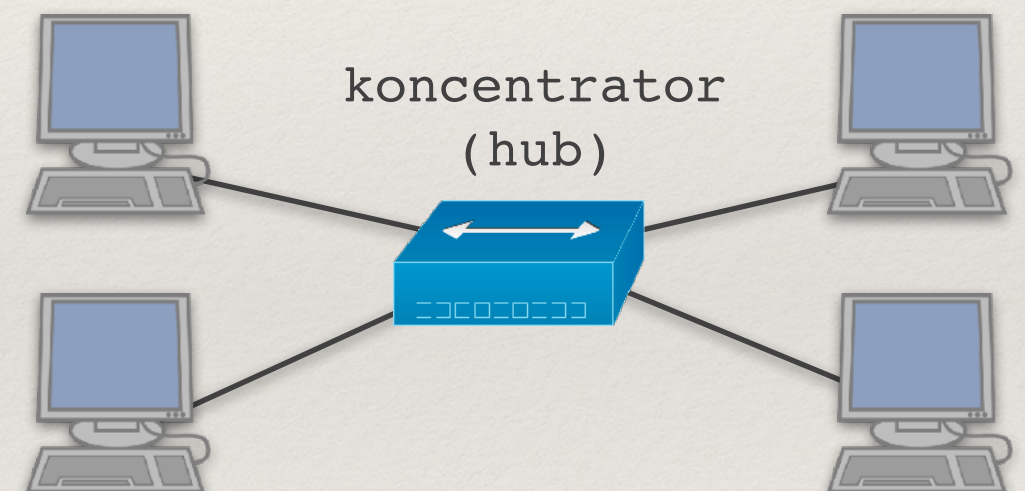
Komunikacja półdupleksowa.



# Połączenia wielopunktowe



- ❖ Wiele urządzeń podpiętych do tego samego kanału komunikacyjnego.
- ❖ Połączenie półdupleksowe.
- ❖ **Jak zapewnić, że tylko jedno urządzenie nadaje?**





---

# Współdzielony kanał

---



# Właściwości

---

- ❖ 1 komputer nadaje  $\rightarrow$  wszyscy go słyszą.
- ❖  $\geq 2$  komputery nadają jednocześnie  $\rightarrow$  zakłócony sygnał.
  - ✦ Kolizje (sieci przewodowe).
  - ✦ Interferencje (sieci bezprzewodowe).
  - ✦ Zazwyczaj nie można wtedy odczytać komunikatu.
- ❖ Brak dodatkowego kanału na komunikaty kontrolne.



# Podejścia deterministyczne

---

## Oparte na wybranym jednym komputerze

- ❖ Jeden komputer odpytuje pozostałe komputery.
- ❖ Decyduje, ile czasu mają nadawać.
- ❖ TDMA (*time division multiple access*): Bluetooth, sieci 2G i 4G

## Oparte na przekazywaniu żetonu

- ❖ Skomplikowane i podatne na błędy implementacyjne.
- ❖ Gubienie żetonu, duplikacja żetonu, ...



# Podejście losowe #1: rundowy ALOHA

---

- ❖ Czas podzielony na rundy.
  - ♦ Długość rundy wystarcza do nadania jednej ramki.
- ❖ Jeśli komputer ma ramkę danych do wysłania, wysyła ją z ppb.  $p$ .
- ❖ Dla  $p = 1/n$ , gdzie  $n$  = liczba komputerów, które chcą wysłać ramkę, sukces średnio co  $e \sim 2,71$  rund (dla dużych  $n \rightarrow$  ćwiczenie)
- ❖ **Problemy:**
  - ♦ Musimy znać  $n$ , żeby wybrać optymalne  $p$ .
  - ♦ Potrzebujemy synchronizacji rund (globalnego zegara).



# Podejście losowe #2: (bezrundowy) ALOHA

---

- ❖ Brak synchronizacji (globalnego zegara): każdy komputer ma swoje rundy.
- ❖ Przy  $p = 1/n$ , wykorzystanie łącza dwukrotnie niższe (ok.  $1 / (2e)$ ).
- ❖ Wciąż musimy znać  $n$ , żeby wybrać optymalne  $p$ .



# Podjęcie losowe #3: oczekiwanie wykładnicze

---

- ❖ Brak synchronizacji: każdy komputer ma swoje rundy.
- ❖ Idea: zmniejszamy ppb. wysłania ramki po nieudanym wysłaniu.
- ❖ Stosowane w Ethernetie i WiFi.
- ❖ Początkowo  $m = 1$ , następnie:
  - ♦ wylosuj  $k$  ze zbioru  $\{ 0, \dots, 2^m - 1 \}$ , odczekaj  $k$  rund i spróbuj wysłać ramkę;
  - ♦ po nieudanym wysłaniu:  $m \leftarrow m + 1$



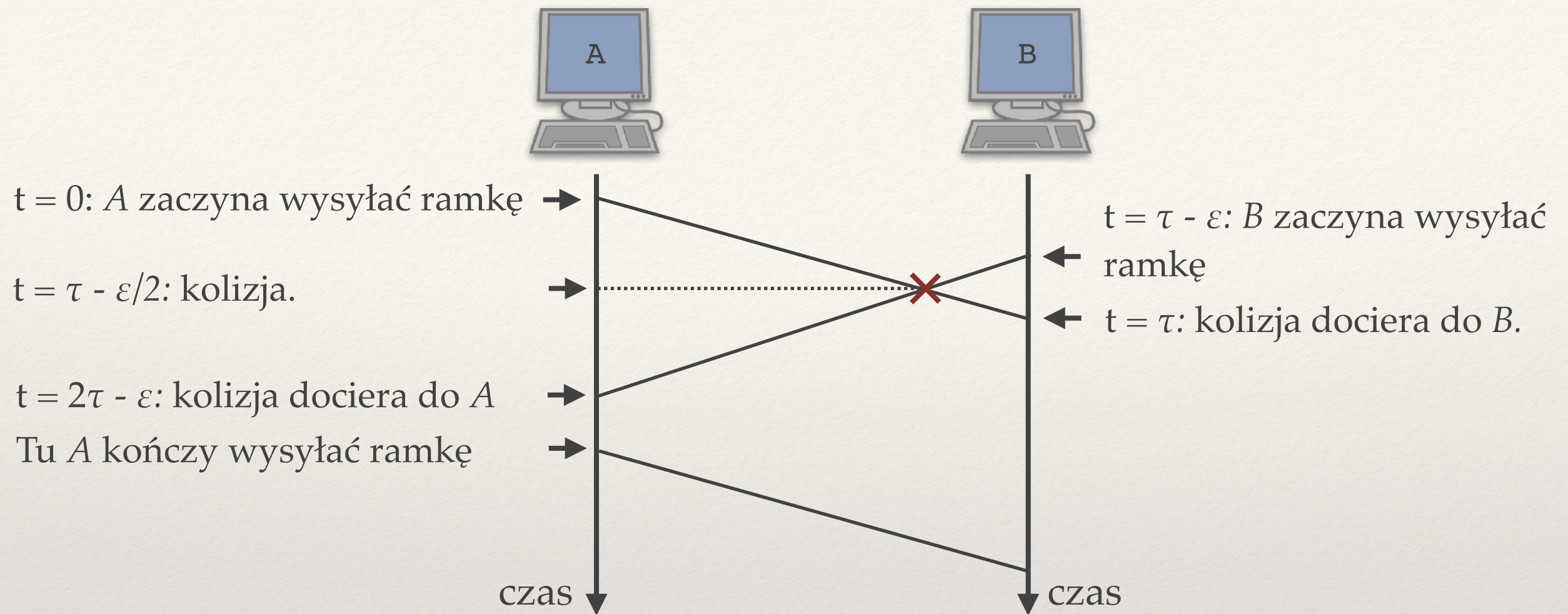
# Skąd wiemy, że nie udało się wysłać ramki?

---

- ❖ **Wariant # 1:** umiemy wykrywać kiedy nastąpiła kolizja (np. Ethernet)
  - ♦ Problem: kolizja też potrzebuje czasu na dotarcie do nadawcy.
- ❖ **Wariant # 2:** brak możliwości wykrywania kolizji (np. WiFi).
- ❖ **Potwierdzanie ramek** (i ich retransmisja w przypadku braku potwierdzenia).
  - ♦ W praktyce potwierdzanie tylko w wariancie #2.



# Interpretacja kolizji

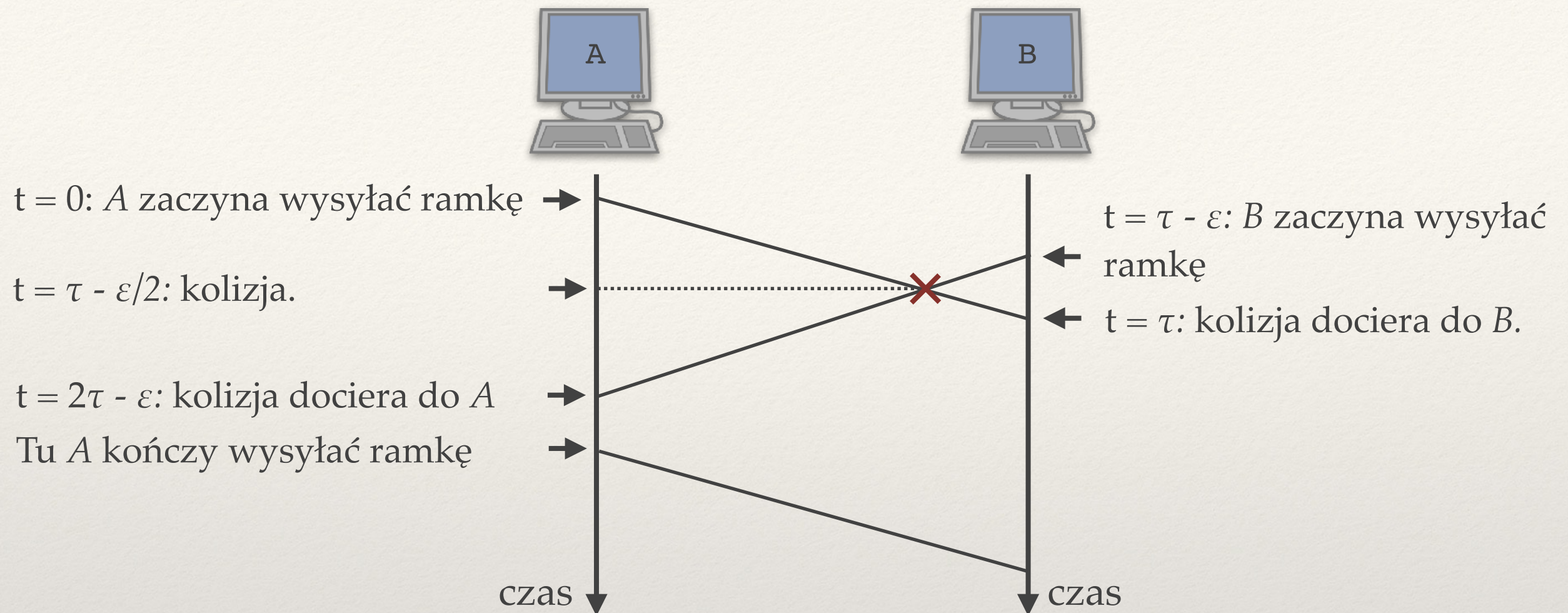


- ❖  $\tau$  = czas propagacji.
- ❖ Załóżmy, że czas wysłania ramki  $\geq 2\tau$

Wtedy jeśli ramka nie dotrze do odbiorcy, to dowiemy się o tym (poprzez kolizję) jeszcze w trakcie jej nadawania



# Interpretacja kolizji



- ❖  $\tau$  = czas propagacji.
- ❖ Załóżmy, że czas wysłania ramki  $\geq 2\tau$

Jak to zapewnić?

Wtedy jeśli ramka nie dotrze do odbiorcy, to dowiemy się o tym (poprzez kolizję) jeszcze w trakcie jej nadawania



# Interpretacja kolizji: Ethernet

---

- ❖ Jak zapewnić, że czas wysłania ramki  $\geq 2 \cdot$  czas propagacji?
- ❖ Ethernet definiuje:
  - ❖ **max. odległość w sieci oraz**
  - ❖ **min. długość ramki**
  - ❖ np. w wariancie 100 Mbit: 100 m i 64 bajty.



# Usprawnienia

---

- ❖ **Carrier sense:** na początku sprawdzamy, czy kanał jest wolny; nie rozpoczynamy nadawania, jeśli słyszymy transmisję.
- ❖ **Rundy są krótsze** niż czas nadawania całej ramki.
- ❖ **Ethernet:** CSMA / CD (*Carrier Sense Multiple Access with Collision Detection*)
  - ✦ Jeśli zauważymy kolizję, przerywamy nadawanie ramki.
- ❖ **WiFi:** CSMA / CA (*Carrier Sense Multiple Access with Collision Avoidance*)
  - ✦ Brak wykrywania kolizji, ramki zawsze nadawane do końca.
  - ✦ Losowe odczekiwanie również przed pierwszą próbą transmisji ramki.



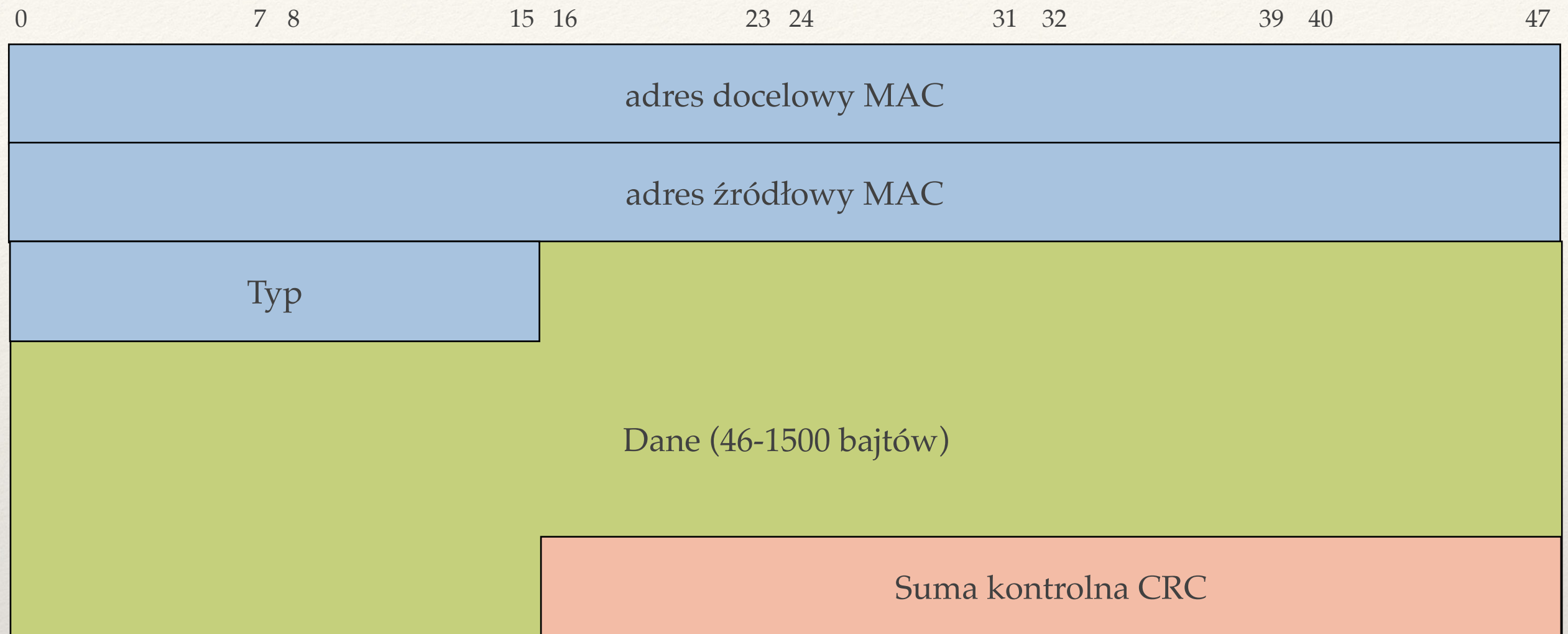
---

# Ramki i adresowanie

---



# Budowa ramki ethernetowej



- ❖ Dane = pakiet otrzymany z warstwy sieciowej.
- ❖ MTU = maksymalny rozmiar tych danych.
- ❖ Typ = identyfikuje protokół w danych, np.  $0x0800 = \text{IP}$ .



# Długość ramki

---

- ❖ MTU  $\leq$  1500 bajtów:
  - ♦ mniejsze ramki mniej podatne na uszkodzenia.
  
- ❖ rozmiar ramki  $\geq$  64 bajty  $\rightarrow$  MTU  $\geq$  46 bajtów:
  - ♦ wypełnienie jeśli za mało danych;
  - ♦ wysyłanie trwa co najmniej  $2 \cdot$  czas propagacji.



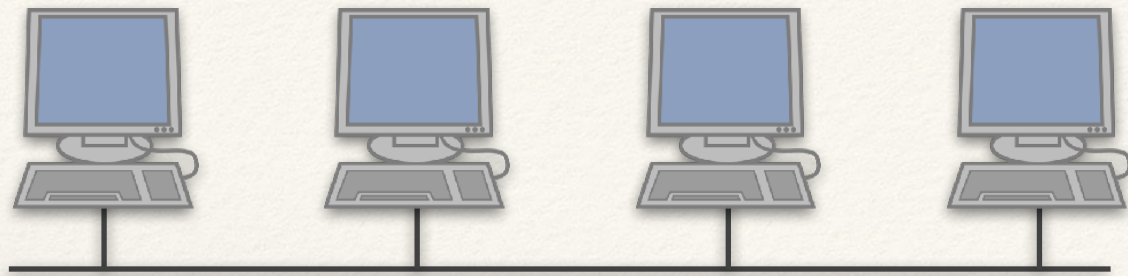
# Adresy ethernetowe (MAC)

---

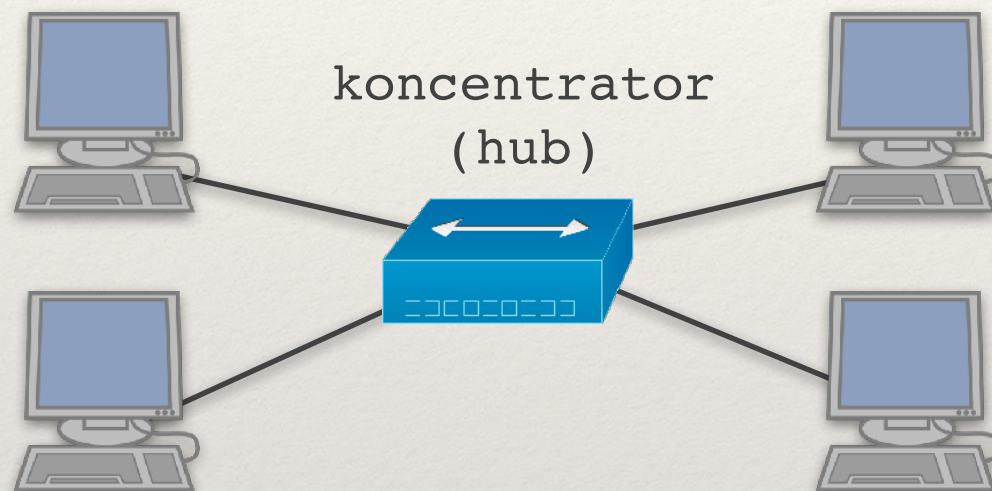
- ❖ 6-bajtowy unikatowy ciąg, przykładowo 00:14:2A:1F:F3:BA.
- ❖ Przypisany (teoretycznie) na stałe do karty sieciowej.
  - ♦ W praktyce można go łatwo zmienić.
- ❖ Pierwsze trzy bajty przyznaje IEEE producentowi kart sieciowych, trzy kolejne nadaje nadaje producent.



# Fizyczna komunikacja w warstwie drugiej



a) wszystko wpięte do wspólnego łącza



b) hub replikuje sygnał na wszystkich portach wyjściowych



c) każdy komputer wysyła ramkę do punktu dostępowego, punkt dostępowy wysyła ją do wszystkich



# Wysyłanie ramek

---

- ❖ Ramka dociera do wszystkich komputerów w sieci.
  - ♦ Nieprawda w przełączanym Ethernetie.
  
- ❖ Przetwarzanie przez kartę sieciową:
  - ♦ Czy nasz adres MAC = adres docelowy ramki
    - ❖ tak → ramka interpretowana, dane ramki → warstwa sieciowa,
    - ❖ nie → ramka wyrzucana.
  - ♦ Karta sieciowa w trybie nasłuchu (*promiscuous mode*) przekazuje do systemu wszystkie widziane ramki (Wireshark).
  - ♦ Rozgłaszanie: jeśli adres odbiorcy = FF:FF:FF:FF:FF:FF, to ramkę interpretują wszyscy.



# MAC vs IP

---

## Jak warstwa sieciowa wysyła pakiety?

- ❖ Z tablicy routingu odczytujemy **kolejny adres IP na trasie do celu:**
  - ♦ albo IP następnego routera na trasie
  - ♦ albo IP docelowego komputera (jeśli leży w naszej sieci).

## Adresowanie

- ❖ Adres źródłowy ramki = adres MAC naszej karty sieciowej.
- ❖ Adres docelowy ramki = adres MAC związany z kolejnym adresem IP na trasie do celu.



# Protokół ARP

---

## ARP = Address Resolution Protocol

- ❖ Rozgłaszamy zapytania „kto ma dany adres IP”.
- ❖ Enkapsulowany w ramach wysyłanych na adres rozgłoszeniowy `FF:FF:FF:FF:FF:FF`
- ❖ Jeden komputer odpowiada.
- ❖ Wszyscy słyszą i zapisują odpowiedź w lokalnej tablicy ARP (na pewien czas).

demonstracja

## IPv6

- ❖ ICMPv6 ma wbudowane tzw. komunikaty *neighbor solicitation* i *neighbor advertisement* zastępujące ARP.



# Rozgłaszanie w warstwie sieciowej

---

- ❖ Pakiet skierowany do adresu rozgłoszeniowego IP:
  - ✦ Umieszczany w ramce adresowanej do `FF:FF:FF:FF:FF:FF`.
  - ✦ Co się stanie, jeśli mamy dwie różne sieci IP działające w tej samej sieci lokalnej?
- ❖ Uwaga na marginesie: podobnie działa translacja multicastowy adres IP → multicastowy adres ethernetowy
  - ✦ np. `224.0.0.9` → `01:00:5e:00:00:09`



# Adresy MAC vs IP

---

- ❖ Dlaczego w warstwie sieciowej nie używamy adresów MAC?
  - ✦ Nie mają hierarchii: tablice routingu byłyby nieużywalnie duże.
- ❖ Dlaczego w warstwie łącza danych nie używamy adresów IP?
  - ✦ Brak możliwości obsługi innych protokołów warstwy sieci.



## Protokół umożliwiający pobieranie adresu IP

- ❖ Zazwyczaj na podstawie adresu MAC dostajemy taki sam adres jak poprzednim razem.
- ❖ Umożliwia też wysyłanie bramy domyślnej, maski sieci, adresów serwerów DNS, ...

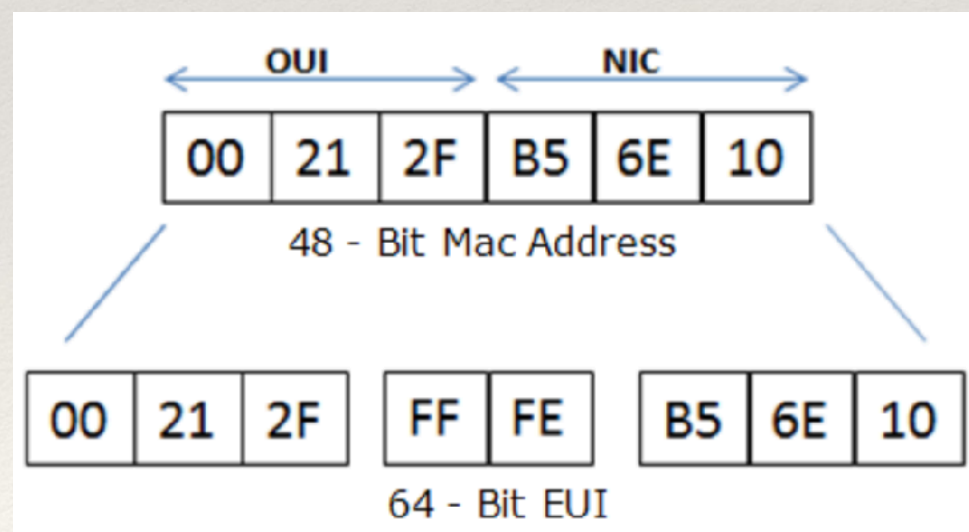
## IPv6

- ❖ ICMPv6 ma wbudowane tzw. komunikaty *router solicitation* i *router advertisement* zastępujące DHCP.



# Konfiguracja automatyczna (bez DHCP)

- ❖ **IPv4:** APIPA = Automatic Private IP Addressing:
  - ♦ komputer losuje adres z sieci `169.254.0.0/16`.
- ❖ **IPv6:** adresy *link-local*
  - ♦ komputer przydziela sobie adres z sieci `fe80::/64`,
  - ♦ ostatnie 64 bity adresu są deterministyczną funkcją adresu MAC





---

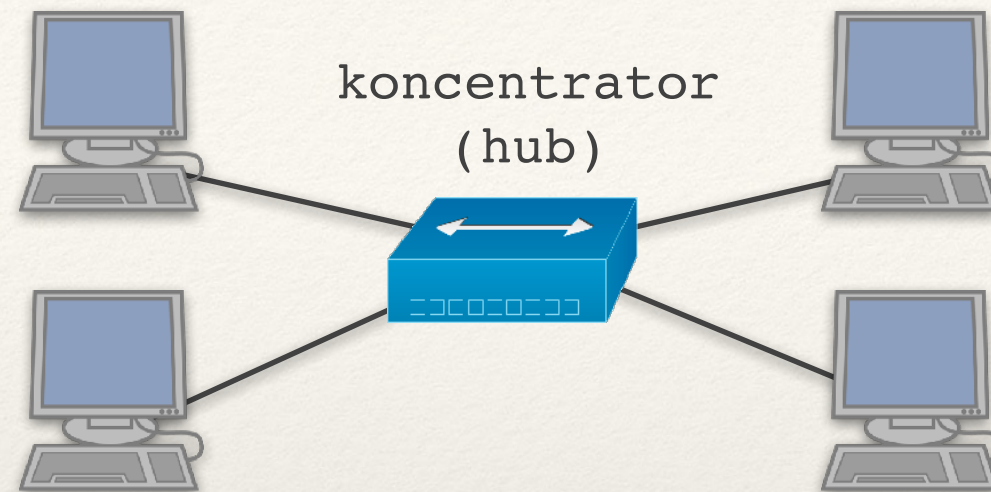
# Przełączanie ramek

---



# Po co?

---

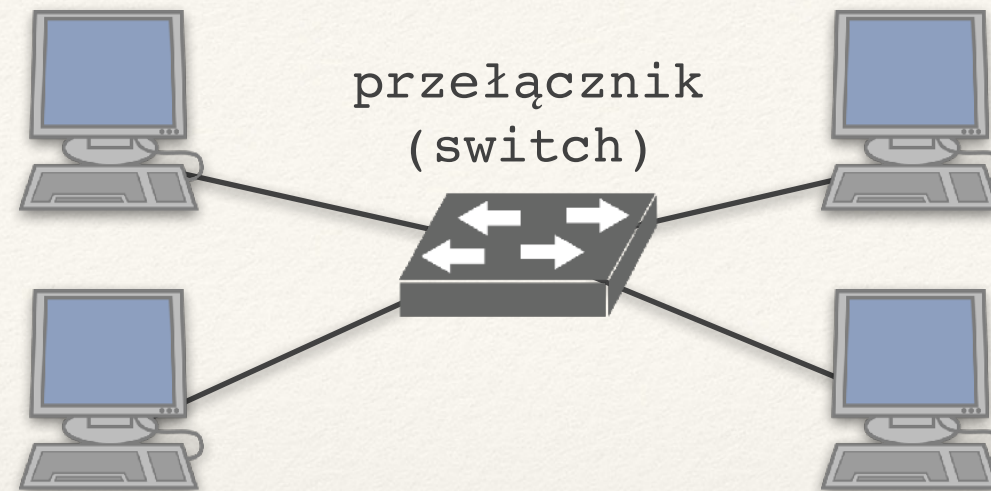


- ❖ Co się stanie jeśli podłączymy do koncentratora 100 komputerów?
  - ♦ Brak prywatności.
  - ♦ Kolizje przechodzą przez koncentrator.



# Przełącznik sieciowy

---



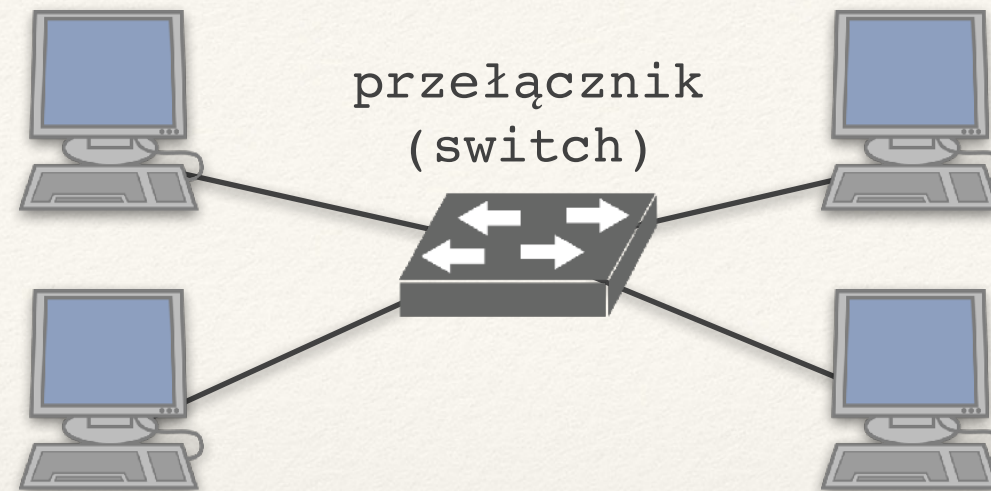
**Przełącznik „rozumie” protokoły warstwy drugiej.**

- ❖ Uczy się w trakcie działania, jakie adresy MAC są podłączone do danych portów.
- ❖ Zazwyczaj do portów podpięte pojedyncze komputery, ale mogą być też sieci.
- ❖ Kolejne transmisje są rozgłaszane do wszystkich portów tylko w razie konieczności.



# Przełącznik sieciowy

---



**Przełącznik „rozumie” protokoły warstwy drugiej.**

- ❖ Uczy się w trakcie działania, jakie adresy MAC są podłączone do danych portów.
- ❖ Zazwyczaj do portów podpięte pojedyncze komputery, ale mogą być też sieci.
- ❖ Kolejne transmisje są rozgłaszane do wszystkich portów tylko w razie konieczności.

**Most = przełącznik z dwoma portami**

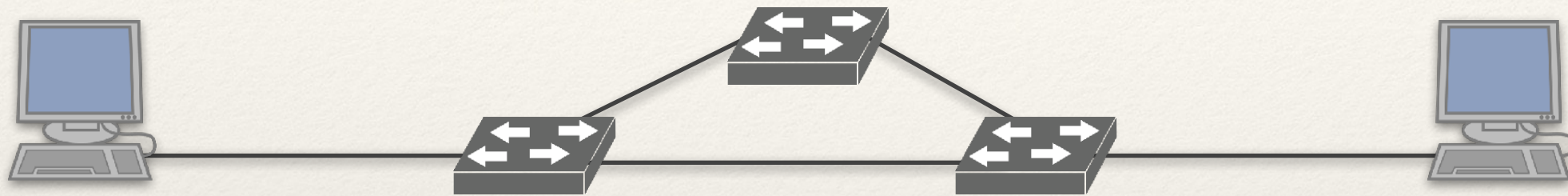
- ❖ Łączy dwie sieci, często różnych technologii (np. Ethernet i WiFi).



# Przełączany Ethernet

---

- ❖ Ramki wysłane na adres rozgłoszeniowy są przekazywane do wszystkich portów.

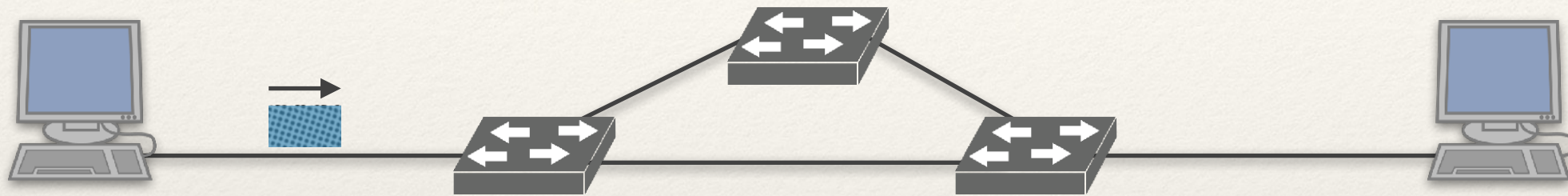




# Przełączany Ethernet

---

- ❖ Ramki wysłane na adres rozgłoszeniowy są przekazywane do wszystkich portów.

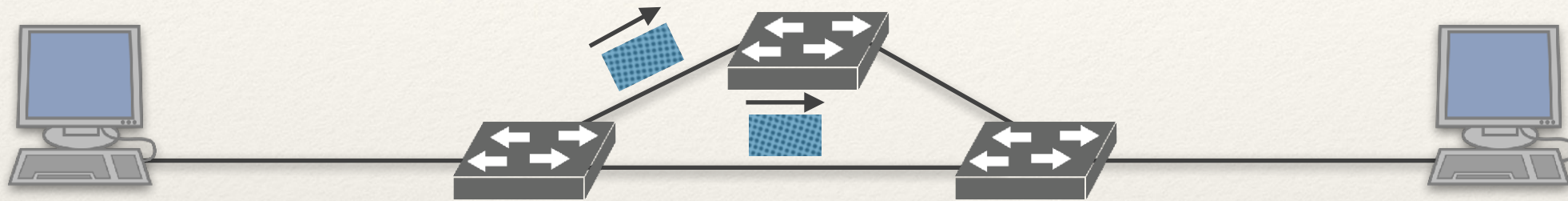




# Przełączany Ethernet

---

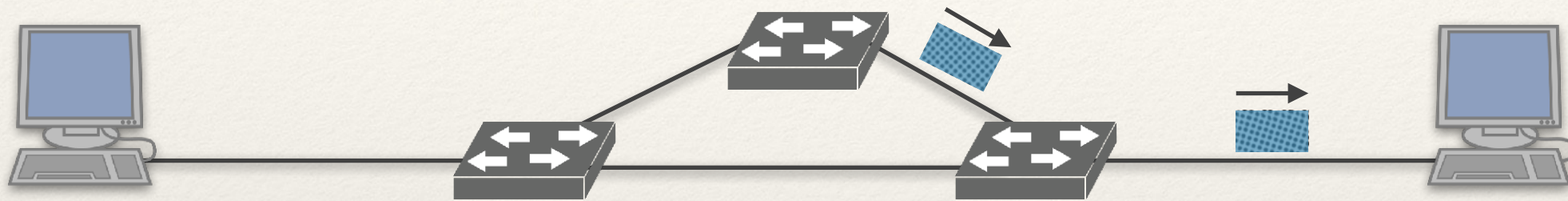
- ❖ Ramki wysłane na adres rozgłoszeniowy są przekazywane do wszystkich portów.





# Przełączany Ethernet

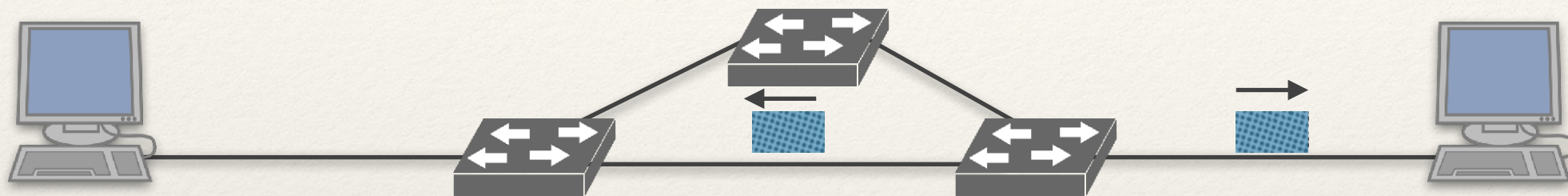
- ❖ Ramki wysłane na adres rozgłoszeniowy są przekazywane do wszystkich portów.





# Przełączany Ethernet

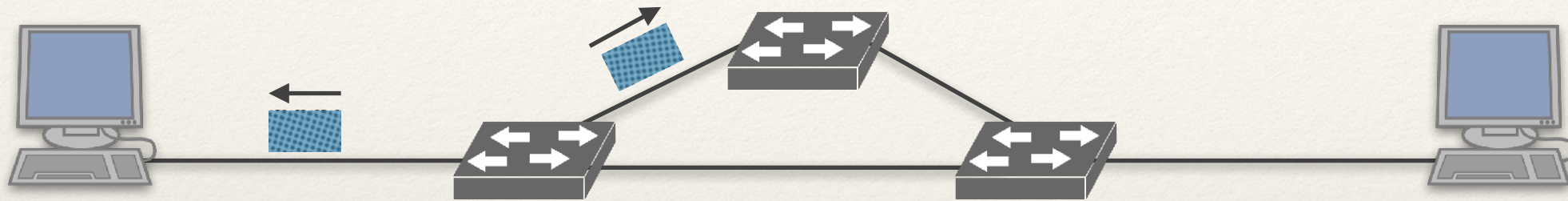
- ❖ Ramki wysłane na adres rozgłoszeniowy są przekazywane do wszystkich portów.





# Przełączany Ethernet

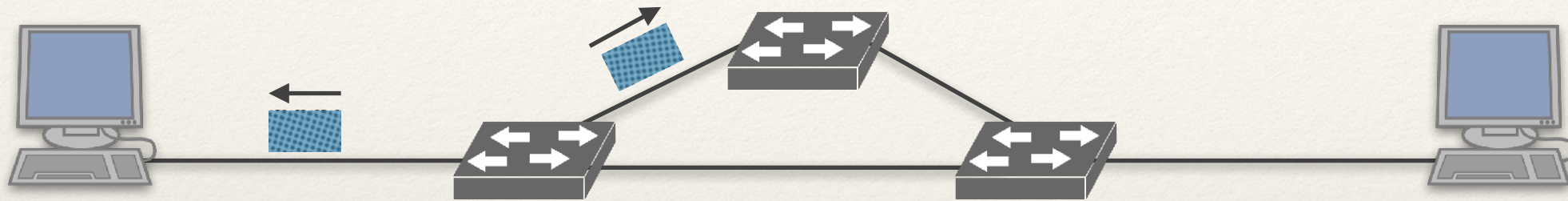
- ❖ Ramki wysłane na adres rozgłoszeniowy są przekazywane do wszystkich portów.





# Przełączany Ethernet

- ❖ Ramki wysłane na adres rozgłoszeniowy są przekazywane do wszystkich portów.

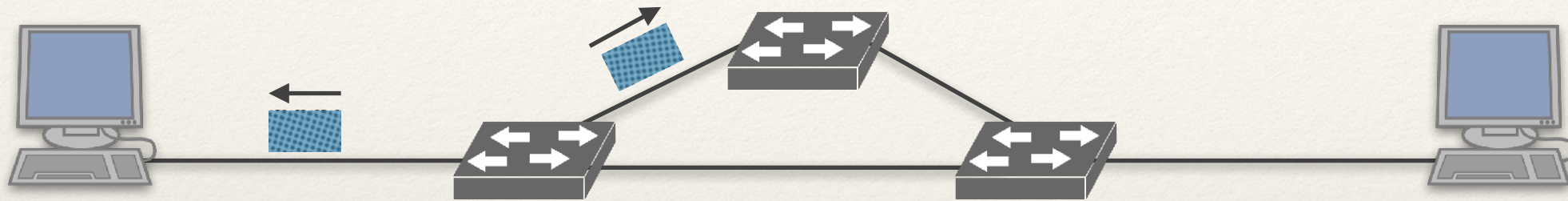


- ❖ Chcemy mieć topologię bez cykli
  - ♦ brak TTL → burze rozgłoszeniowe



# Przełączany Ethernet

- ❖ Ramki wysłane na adres rozgłoszeniowy są przekazywane do wszystkich portów.

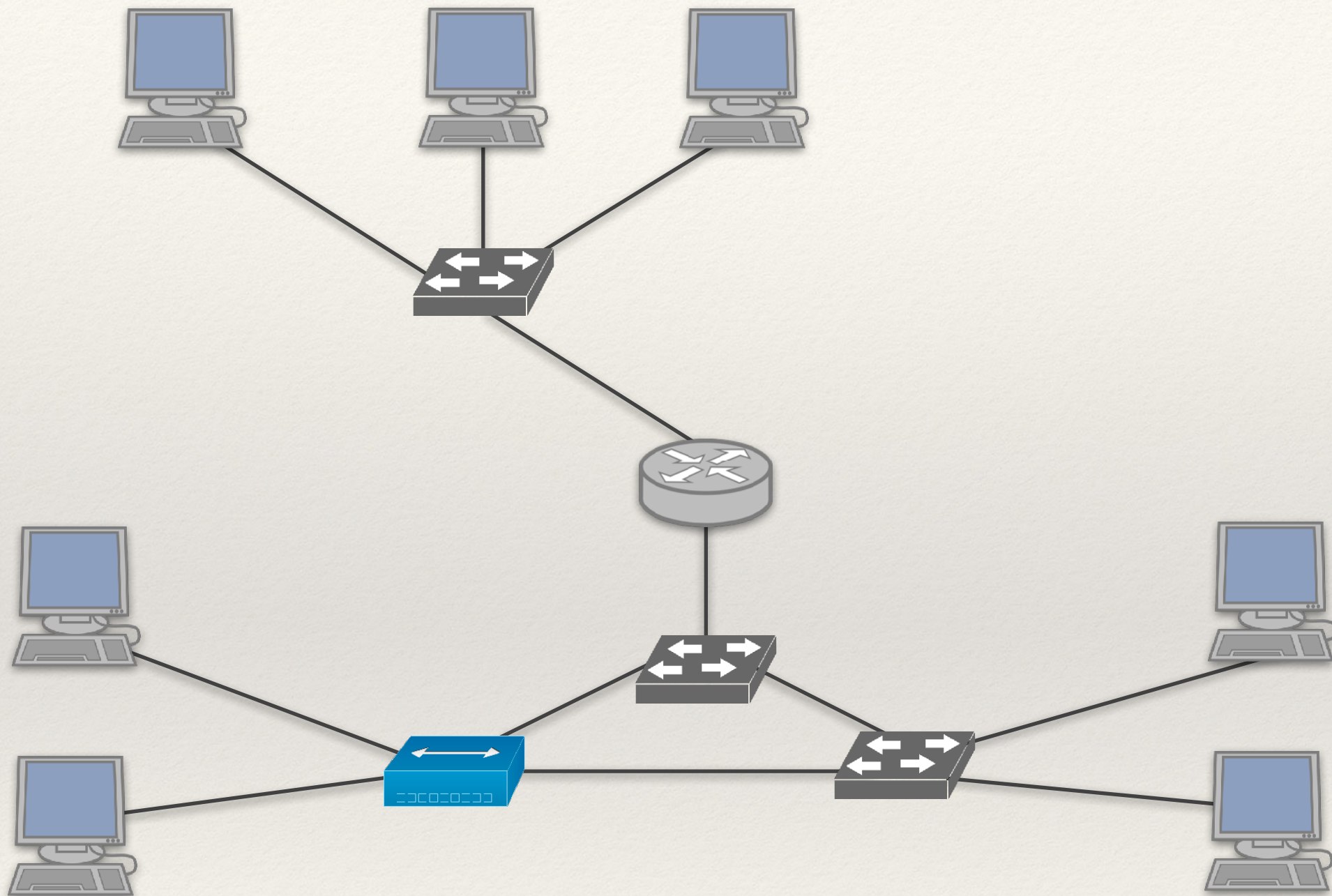


- ❖ Chcemy mieć topologię bez cykli
  - ♦ brak TTL → burze rozgłoszeniowe
- ❖ Przełączniki używają STP (*Spanning Tree Protocol*)
  - ♦ Rozproszony algorytm budowy drzewa spinającego.
  - ♦ Spośród połączeń wybierają drzewo, inne porty wykorzystywane tylko w wypadku awarii.



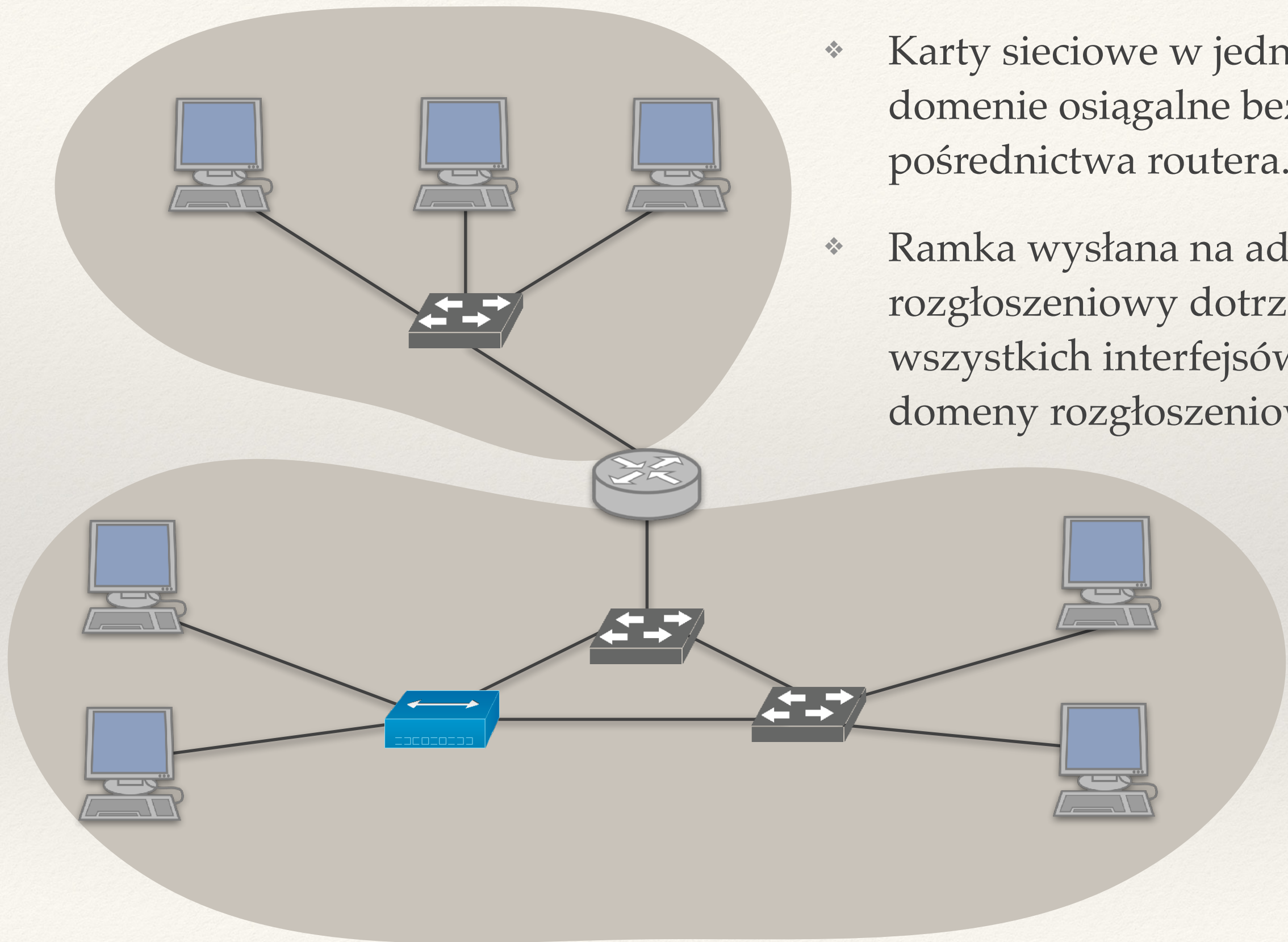
# Domena rozgłoszeniowa

---





# Domena rozgłoszeniowa

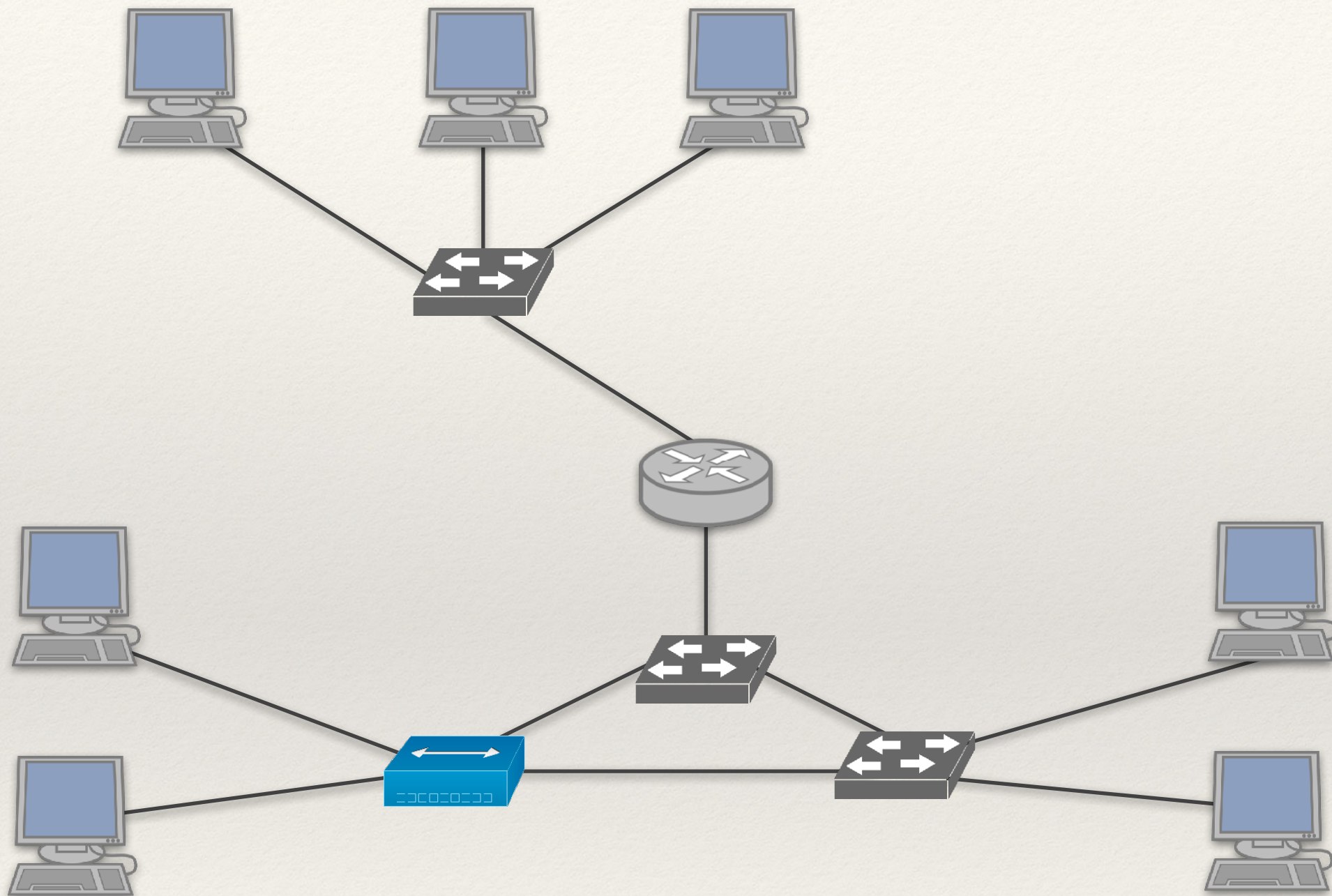


- ❖ Karty sieciowe w jednej domenie osiągalne bez pośrednictwa routera.
- ❖ Ramka wysłana na adres rozgłoszeniowy dotrze do wszystkich interfejsów z danej domeny rozgłoszeniowej.



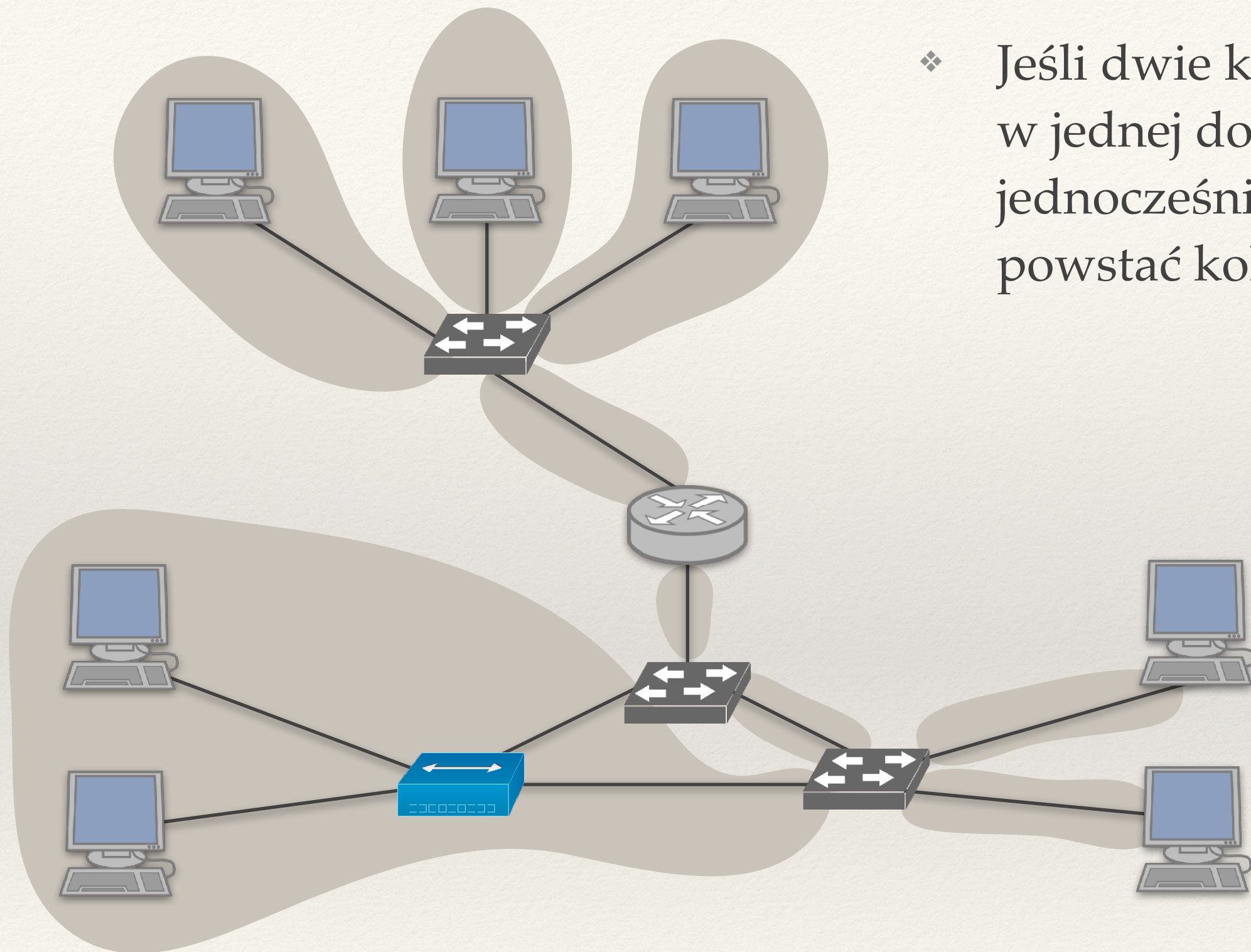
# Domena kolizyjna

---





# Domena kolizyjna

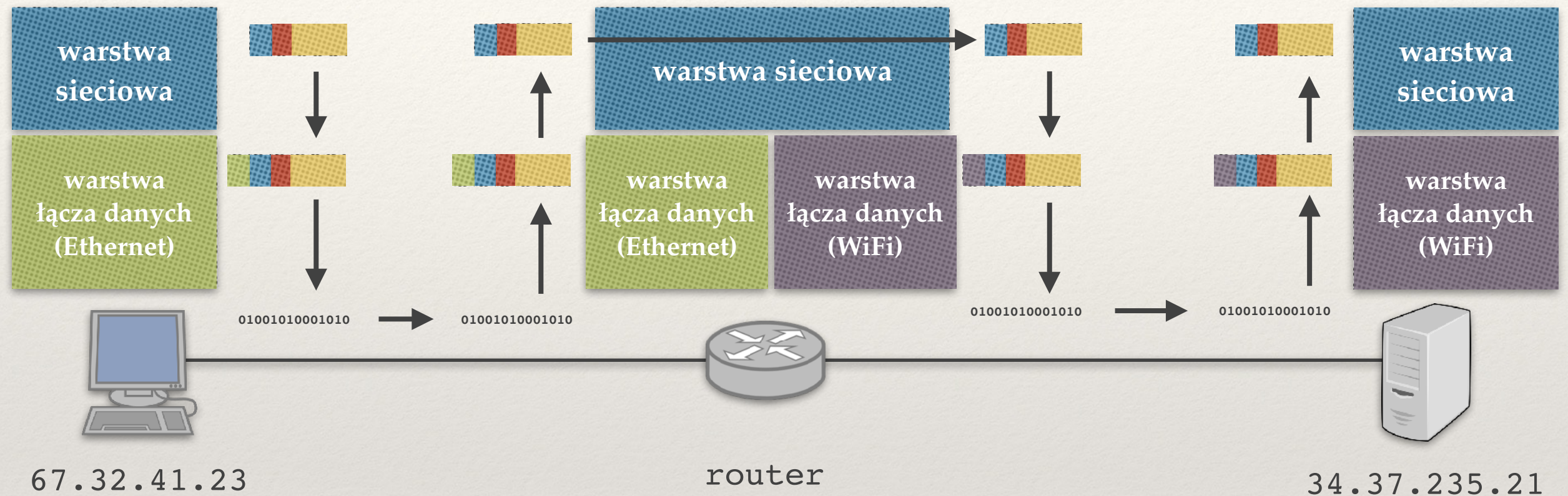


- ❖ Jeśli dwie karty sieciowe w jednej domenie nadają jednocześnie, to może powstać kolizja.



# Łączenie sieci różnych technologii

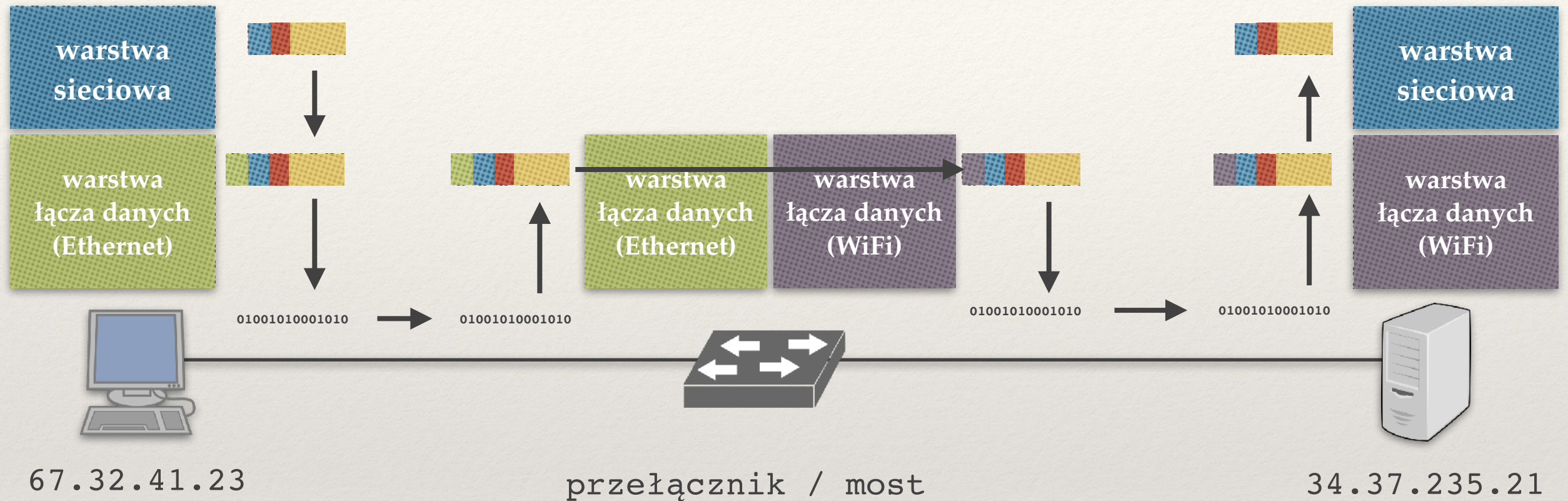
## Opcja 1: łączenie za pomocą routera (już poznaliśmy)





# Łączenie sieci różnych technologii

## Opcja 2: łączenie za pomocą mostu

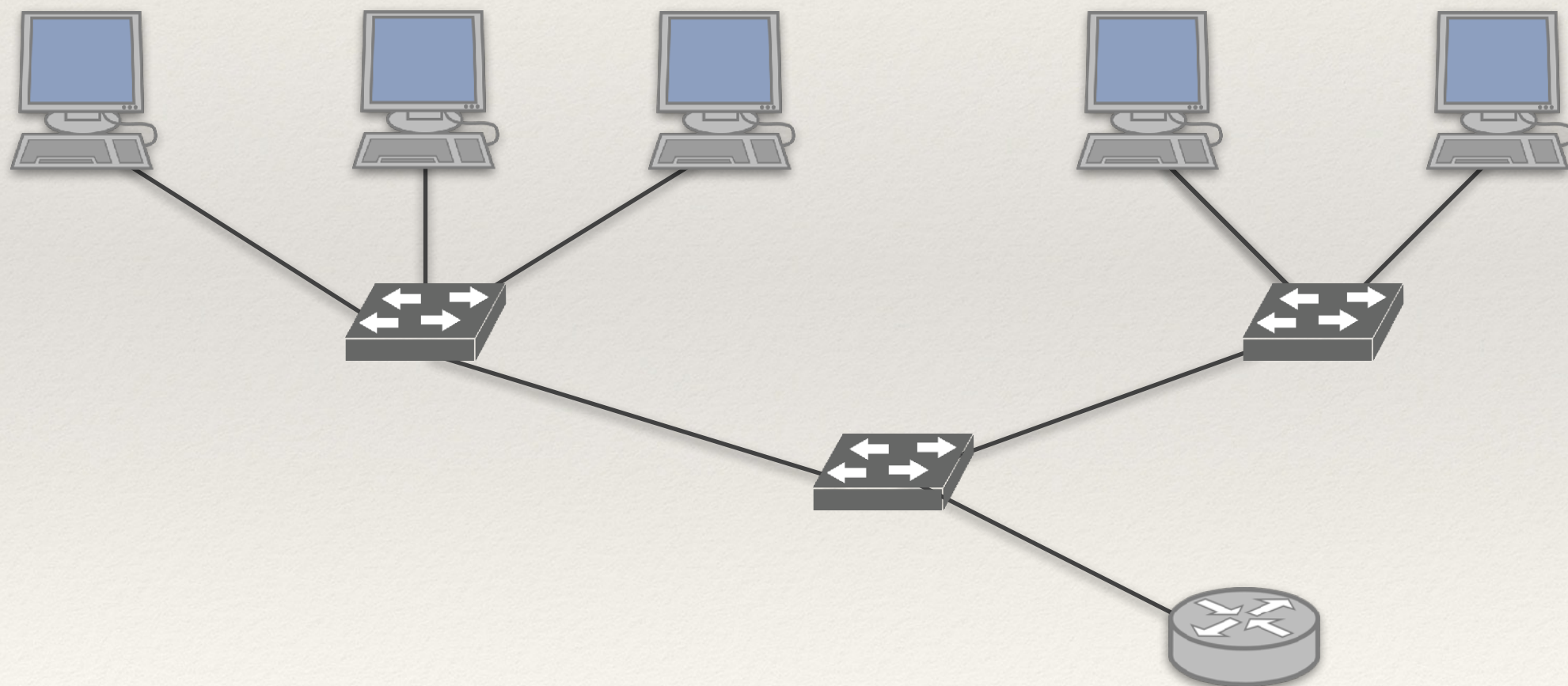


- ❖ Szybsze: nie ma tablicy routingu, tylko podmiana nagłówka + przeliczenie sumy kontrolnej
- ❖ Ale: nie rozumie IP, fragmentacja IP niemożliwa, nie poradzi sobie jeśli pakiet jest za duży w stosunku do docelowego MTU



# VLAN: wirtualne sieci lokalne

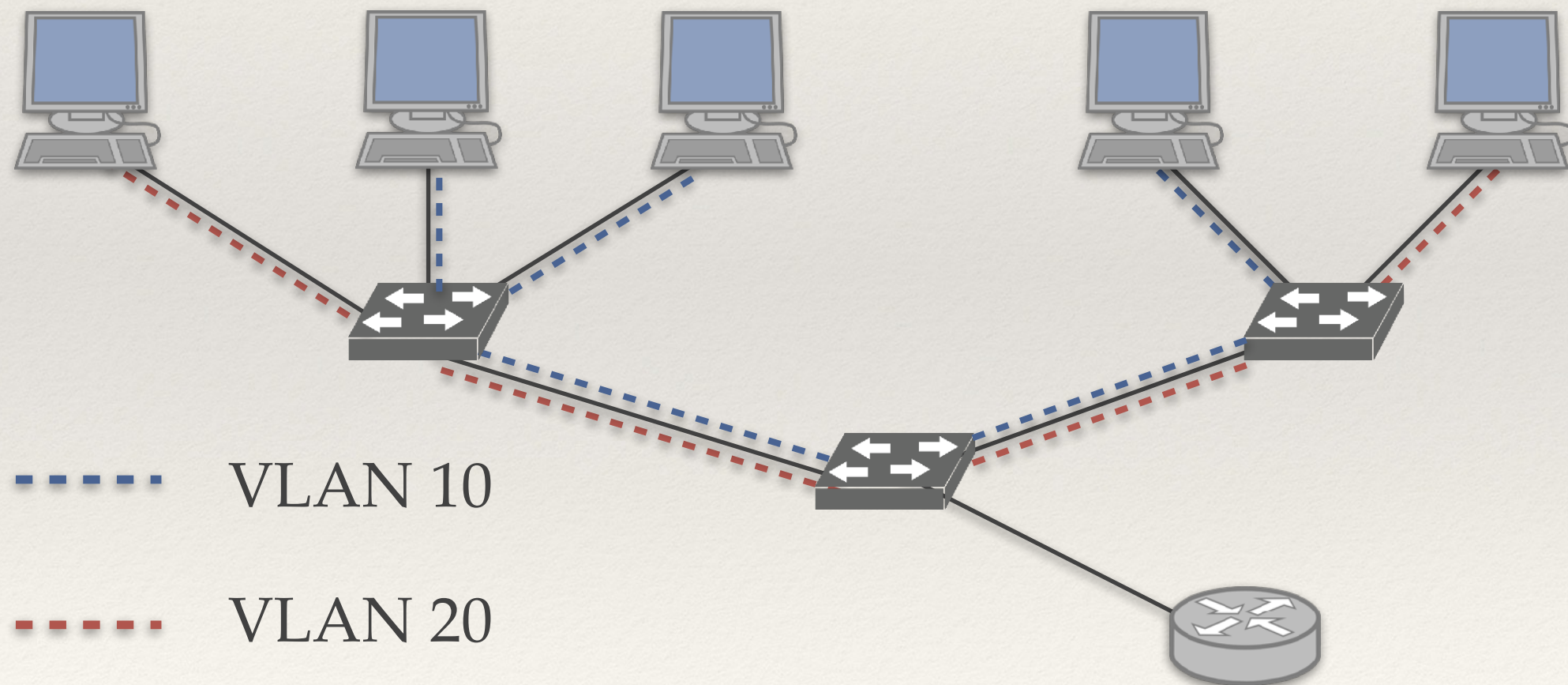
---





# VLAN: wirtualne sieci lokalne

- ❖ Fizyczne połączenie nie musi być tożsame z logiczną konfiguracją.
- ❖ Dla każdego portu przełącznika ustalamy do jakich VLAN-ów należy.
- ❖ W wysyłanych ramkach pojawia się dodatkowe pole będące numerem VLAN-u → przesyłana tylko w obrębie danego VLAN-u.





---

# Sieci bezprzewodowe

---

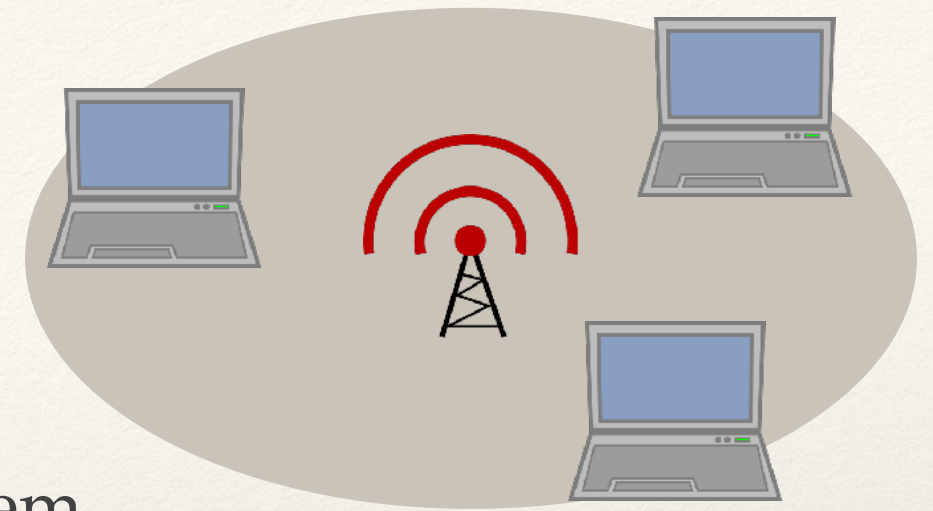


# Sieci WLAN z punktem dostępowym

---

## Punkt dostępowy (access point, AP)

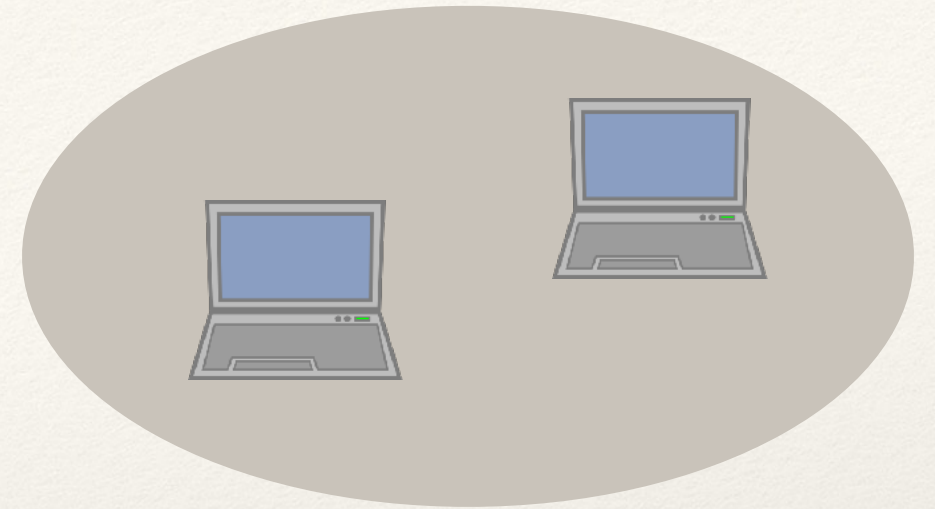
- ❖ Każdy komunikuje się tylko z AP
- ❖ Każdy musi być w zasięgu AP
- ❖ AP jest połączony zazwyczaj kablem z routerem
  - ♦ może pełnić funkcję mostu między sieciami WiFi i Ethernetem,
  - ♦ może też być zintegrowany z routerem.
- ❖ AP rozsyła ramki identyfikacyjne (*beacon frames*) zawierające m.in. nazwę sieci SSID.
- ❖ Przed transmisją trzeba się związać z wybranym AP, opcjonalne uwierzytelnianie.





# Sieci ad-hoc

---



- ❖ Sieci WLAN bez punktu dostępowego
- ❖ Brak routingu = zakładamy, że każde urządzenie jest w zakresie nadawania każdego innego.

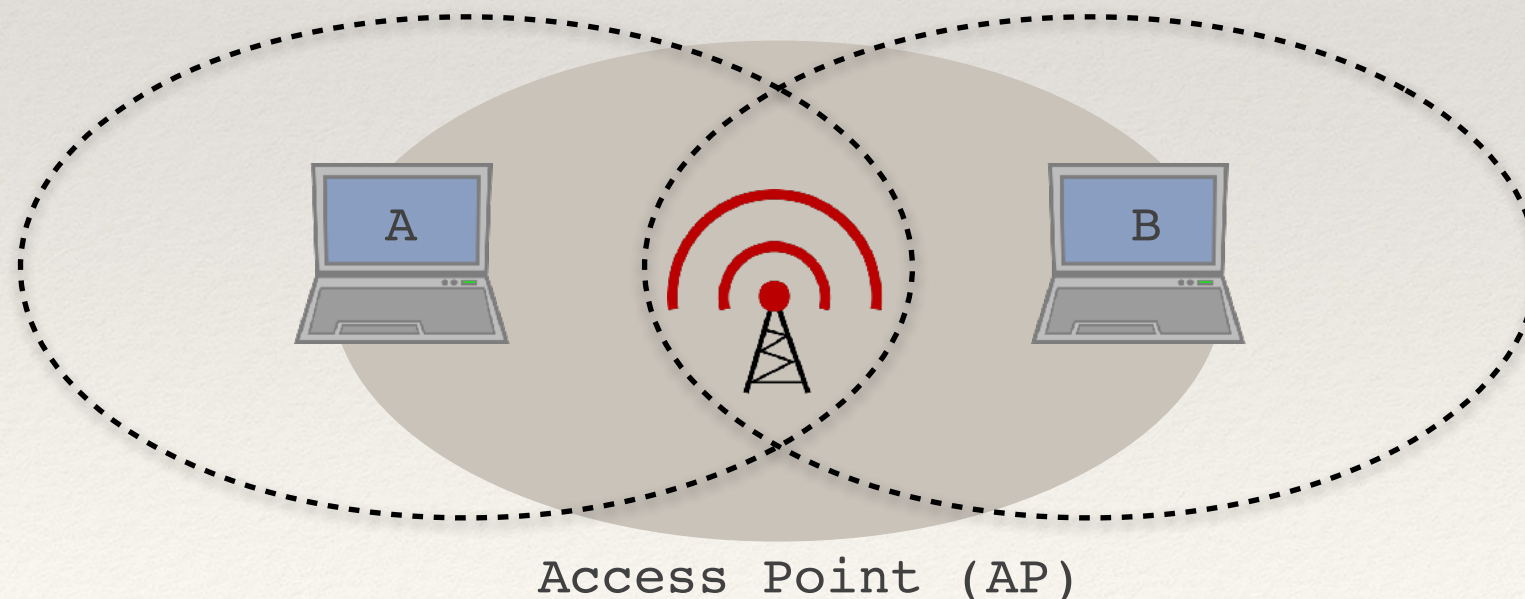


# Problem ukrytej stacji

---

Strategia „nadawaj jeśli nikt nie nadaje” nie zawsze działa

- ❖ A nadaje do AP
- ❖ B chce nadać do AP.
  - ✦ B sprawdza stan kanału.
  - ✦ B nie słyszy żadnej transmisji, więc nadaje.
- ❖ Sygnał od A i B interferuje przy AP.

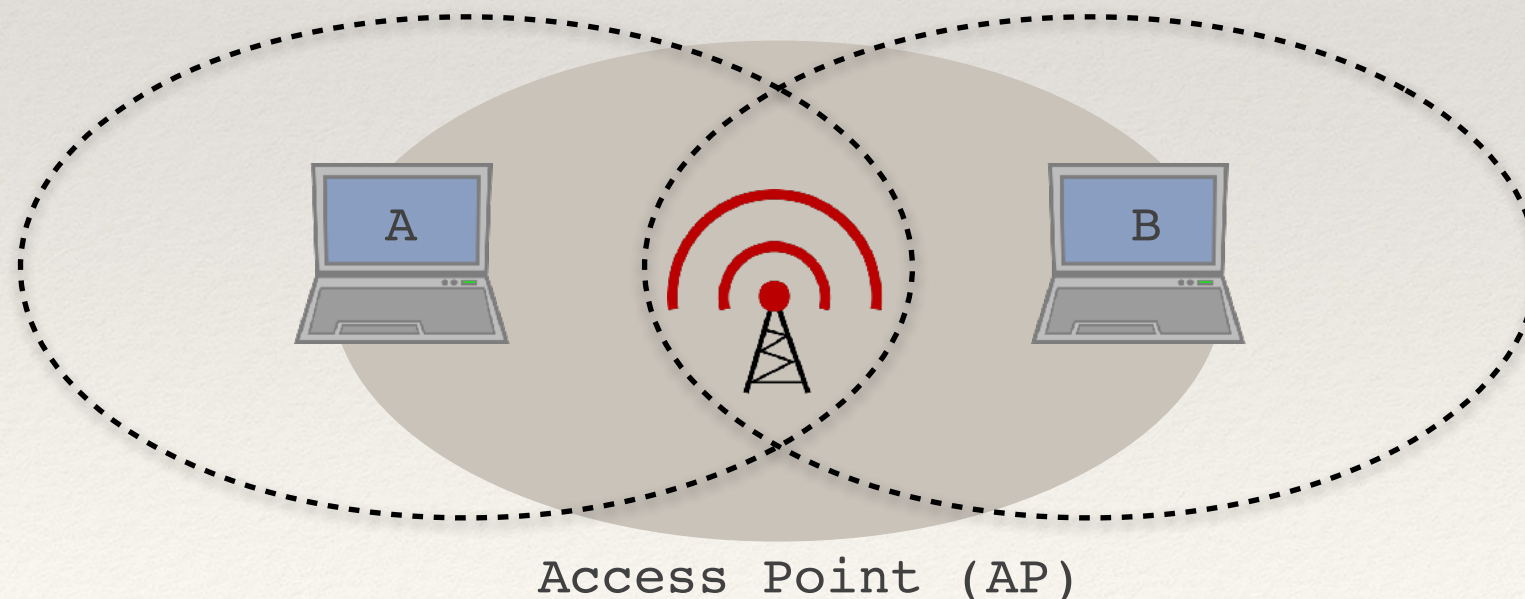




# Problem ukrytej stacji: RTS+CTS

## Rozwiązanie wbudowane w CSMA/CA.

- ❖ Zanim *A* nada ramkę do AP, wysyła komunikat RTS (*Request To Send*).
- ❖ AP odsyła CTS (*Clear To Send*),
  - ♦ *B* również słyszy CTS.
  - ♦ *B* będzie milczeć przez czas potrzebny *A* na wysłanie ramki.
- ❖ *A* wysyła ramkę do AP, AP ją potwierdza.





---

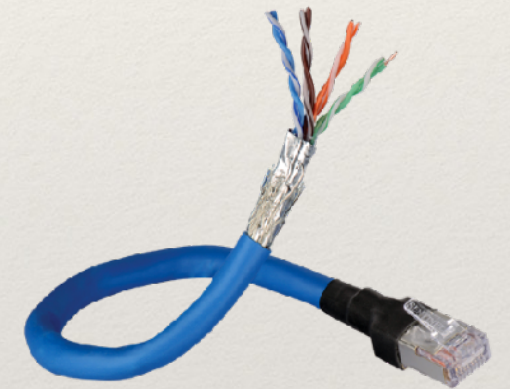
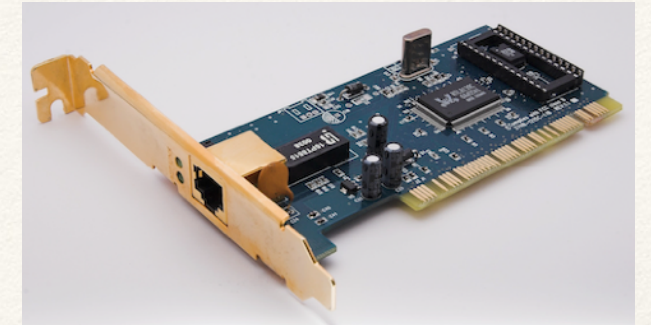
# Warstwa fizyczna

---



# Warianty Ethernetu

- ❖ Karta pracuje z określoną częstotliwością nadawania → szybkość transmisji (w bit/s).
- ❖ **Najczęstsze warianty:**
  - ✦ 100 Mbit/s (Fast Ethernet)
  - ✦ **1 Gbit/s (Gigabit Ethernet)**
  - ✦ **2,5 Gbit/s**
  - ✦ 10 Gbit/sek
- ❖ Zazwyczaj wykorzystuje **skrętkę niekranowaną** (8 żył), rzadziej światłowód.
  - ✦ Do wyższych prędkości potrzebne kable o wyższych kategoriach: kat. 5e do 2,5 Gbit/s, kat. 6 do 10 GBit.

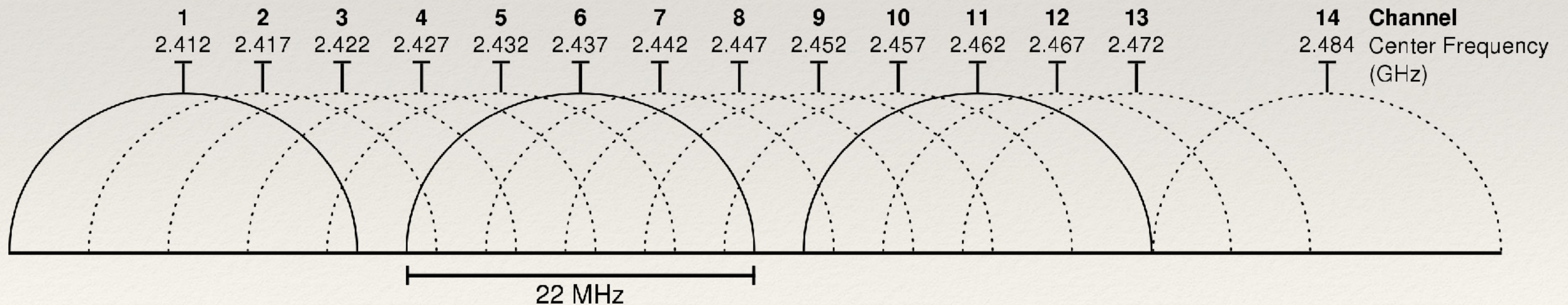




# Sieci bezprzewodowe

Wykorzystują fale radiowe o określonej częstotliwości





- ❖ Nadawca i odbiorca muszą korzystać z tej samej częstotliwości.
- ❖ Trzy pasma (zakresy częstotliwości): 2,4 Ghz, 5 Ghz, 6 Ghz
- ❖ Dostępne do nadawania bez licencji.
- ❖ Przykładowo w paśmie 2,4 Ghz wyróżniono 14 częstotliwości (tzw. kanałów)
- ❖ Urządzenia nadające w kanale X zakłócają transmisje w sąsiednich.



Obrazek ze strony <http://en.wikipedia.org/wiki/802.11>



# Warianty WiFi

Generation	Visual	IEEE standard	Adopted	Maximum link rate (Mbit/s)	Radio frequency (GHz)
—	—	<a href="#">802.11</a>	1997	1–2	2.4
—	—	<a href="#">802.11b</a>	1999	1–11	2.4
—	—	<a href="#">802.11a</a>	1999	6–54	5
—	—	<a href="#">802.11g</a>	2003		2.4
<b>Wi-Fi 4</b>		<a href="#">802.11n</a>	2009	6.5–600	2.4, 5
<b>Wi-Fi 5</b>		<a href="#">802.11ac</a>	2013	6.5–6933	5 <sup>[b]</sup>
<b>Wi-Fi 6</b>		<a href="#">802.11ax</a>	2021	0.4–9608	2.4, 5
<b>Wi-Fi 6E</b>					6 <sup>[c]</sup>
<b>Wi-Fi 7</b>		<a href="#">802.11be</a>	2024 <sup>[d]</sup>	0.4–23,059	2.4, 5, 6
<b>Wi-Fi 8<sup>[45][46]</sup></b>	—	<a href="#">802.11bn</a>		100,000	2.4, 5, 6

- ❖ WiFi 4 i późniejsze: większe prędkości wymagają wielu anten.
- ❖ Nagłówek ramki przesyłany jest z minimalną prędkością dopuszczoną dla danego standardu



# Problemy z warstwą fizyczną

---

## ❖ Malejąca siła sygnału

- ♦ Zwłaszcza w WiFi: sygnał rozchodzi się wielokierunkowo, słabnie lub zanika przy przechodzeniu przez ściany.
- ♦ Zasięg WiFi: ok. 50 m (2,4 Ghz) i ok. 20 m (5 Ghz).

## ❖ Interferencje / kolizje

- ♦ Współcześnie głównie w sieciach bezprzewodowych.
- ♦ Interferencje z kartami sieciowymi, kuchenkami mikrofalowymi, Bluetoothem.
- ♦ Propagacja wielościeżkowa: ten sam sygnał wędruje do celu ścieżkami różnej długości i interferuje ze sobą.



# Lektura dodatkowa

---

- ❖ Kurose & Ross: rozdział 6 i 7.
- ❖ Tanenbaum: rozdział 4.



# Zagadnienia

---

- ❖ Jakie są zadania warstwy łącza danych a jakie warstwy fizycznej?
- ❖ Czym różni się koncentrator od przełącznika sieciowego?
- ❖ Jak działa algorytm rundowy i bezrundowy ALOHA?
- ❖ Jak działa algorytm odczekiwania wykładniczego?
- ❖ Wyjaśnij skróty CSMA/CD i CSMA/CA.
- ❖ Opisz budowę ramki Ethernetowej.
- ❖ Co to jest adres MAC?
- ❖ Do czego służy tryb nasłuchu (*promiscuous mode*)?
- ❖ Po co w Ethernetie definiuje się minimalną długość ramki?
- ❖ Do czego służą protokoły ARP i DHCP?
- ❖ Czym różni się łączenie dwóch sieci za pomocą mostu od łączenia ich za pomocą routera?
- ❖ Jak warstwa łącza danych realizuje rozgłaszanie?
- ❖ Na czym polega tryb uczenia się w przełączniku sieciowym?
- ❖ Po co w przełączanym Ethernetie stosuje się algorytm drzewa spinającego?
- ❖ Co to jest sieć VLAN? Po co się ją stosuje?
- ❖ Wyjaśnij zjawisko ukrytej stacji.
- ❖ Na czym polega rezerwowanie łącza za pomocą RTS i CTS?