



## Podstawy Sieci Komputerowych

### Wprowadzenie do sieci komputerowych

Modele warstwowe. Rodzaje sieci teleinformatycznych.

Urządzenia sieci teleinformatycznych

dr hab. inż. Konrad Gromaszek



# Wprowadzenie

rosnąca rola sieci komputerowych

## • Rewolucje przemysłowe

Pierwsza rewolucja  
przemysłowa  
(Industry 1.0)



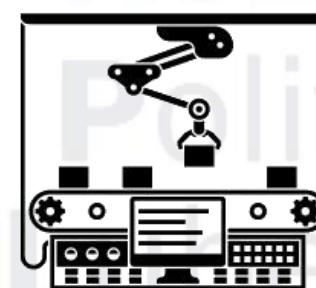
XVIII w.  
maszyna parowa i  
mechanizacja  
produkcyjna

Druga rewolucja  
przemysłowa  
(Industry 2.0)



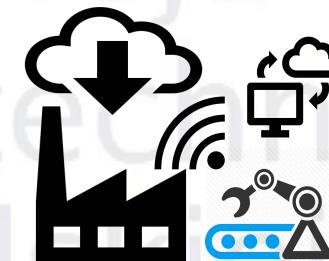
XIX w.  
wynalezienie  
elektryczności i linii  
montażowej

Trzecia rewolucja  
przemysłowa  
(Industry 3.0)



Lata 70' XX w.  
Wdrożenie częściowej  
automatyzacji  
produkcyjnej za pomocą  
PLC i komputerów

Czwarta rewolucja  
przemysłowa  
(Industry 4.0)



XX w.  
Wykorzystanie technologii  
informacyjnych i  
komunikacyjnych  
w przemyśle

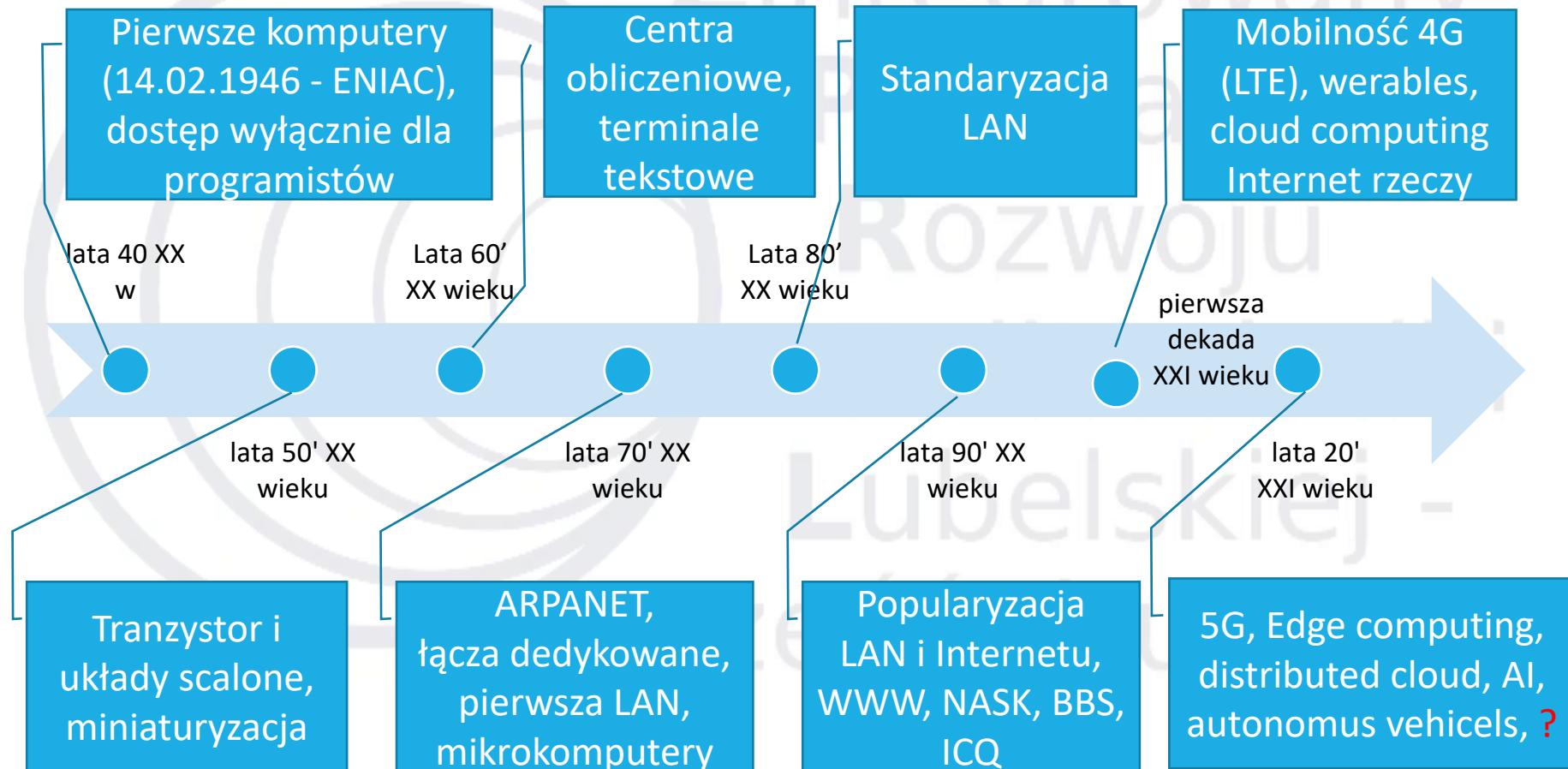
# Wprowadzenie

- Wpływ łączenia hostów i komunikacji
  - Model pojedynczego komputera
  - Model "pogrupowanych" systemów komputerowych
  - Odrębne systemy dla różnych usług
  - Sieci konwergentne
  - Sieci kablowe vs. bezprzewodowe
  - Wirtualizacja usług
  - „Infrastruktura czy chmura?”

# Podstawowe definicje

- Sieć komputerowa to medium umożliwiające połączenie dwóch lub więcej komputerów w celu wzajemnego komunikowania się.
- Cele tworzenia sieci
- Zastosowania sieci
- Rodzaje sieci teleinformatycznych

# Tło historyczne rozwoju sieci komputerowych



# Składniki sieci



# Rodzaje komunikacji

- Komunikacja z ***komutacją połączeń***
  - Strony nawiązują połączenie, dla którego rezerwowane są zasoby na wszystkich stacjach pośredniczących na czas trwania połączenia (Przykłady zastosowań: telefonia, radiofonia, telewizja)
- Komunikacja z ***komutacją pakietów***
  - Strony wysyłają dane w formie niezależnie przesyłanych pakietów, kiedy uznają to za stosowne. Po przesłaniu pakietu, wszystkie zasoby są zwalniane. (Przykład: większość klasycznych sieci LAN)
- Metody pośrednie
  - Metody, które próbują łączyć cechy obu powyższych podejść. (Przykład: ISDN)

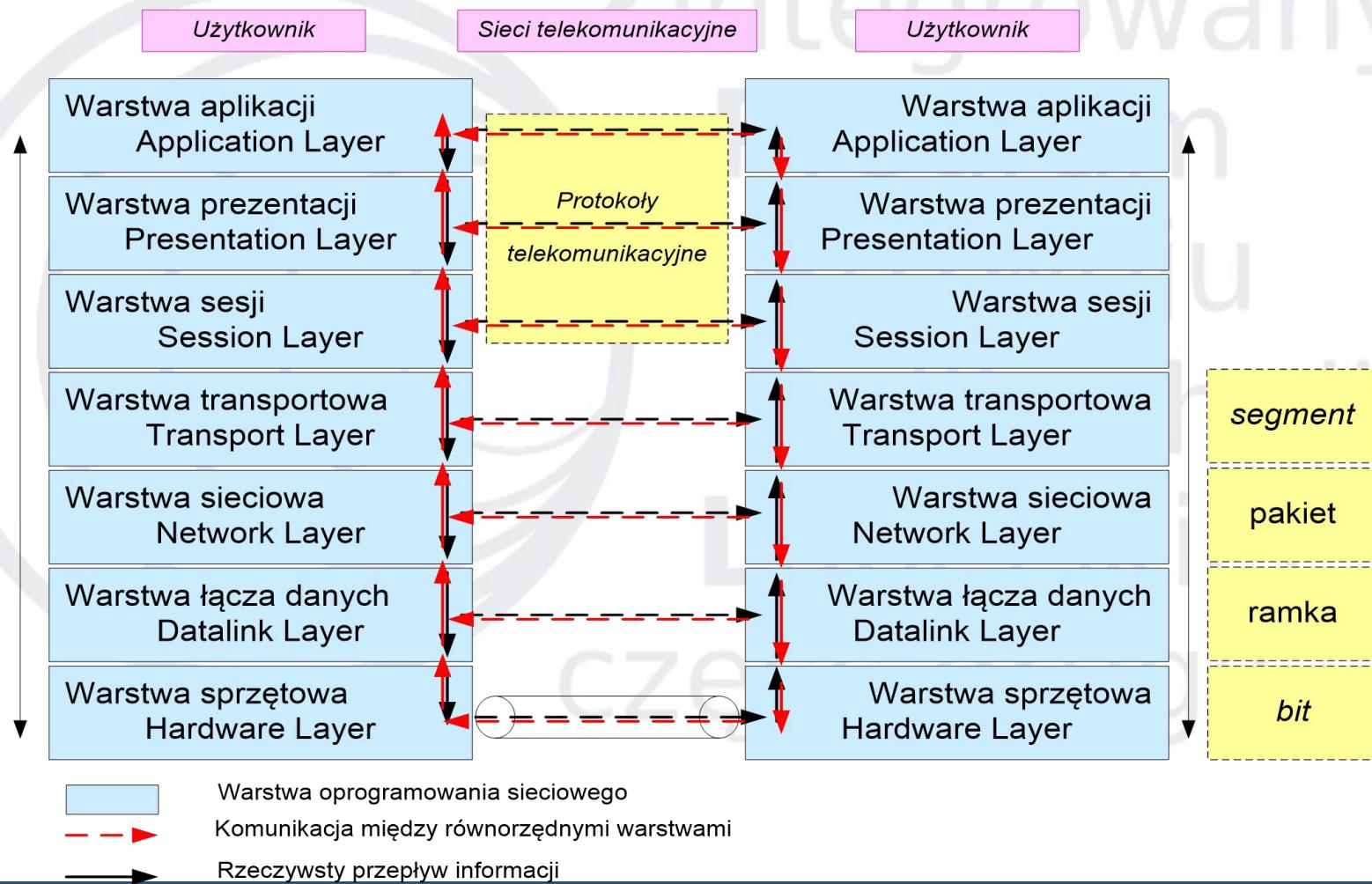
# Sieciowe modele warstwowe

- Podstawowym założeniem modeli warstwowych jest podział całego zagadnienia komunikacji sieciowej na szereg współpracujących ze sobą warstw (ang. *layers*)
- Każda z nich może być tworzona przez programistów zupełnie niezależnie, przy zapewnieniu protokołów według których wymieniają się one informacjami
- W rezultacie, na każdej warstwie powstaje pewien standard transmisji określający format przesyłanych danych (segment, pakiet, ramka itd. )

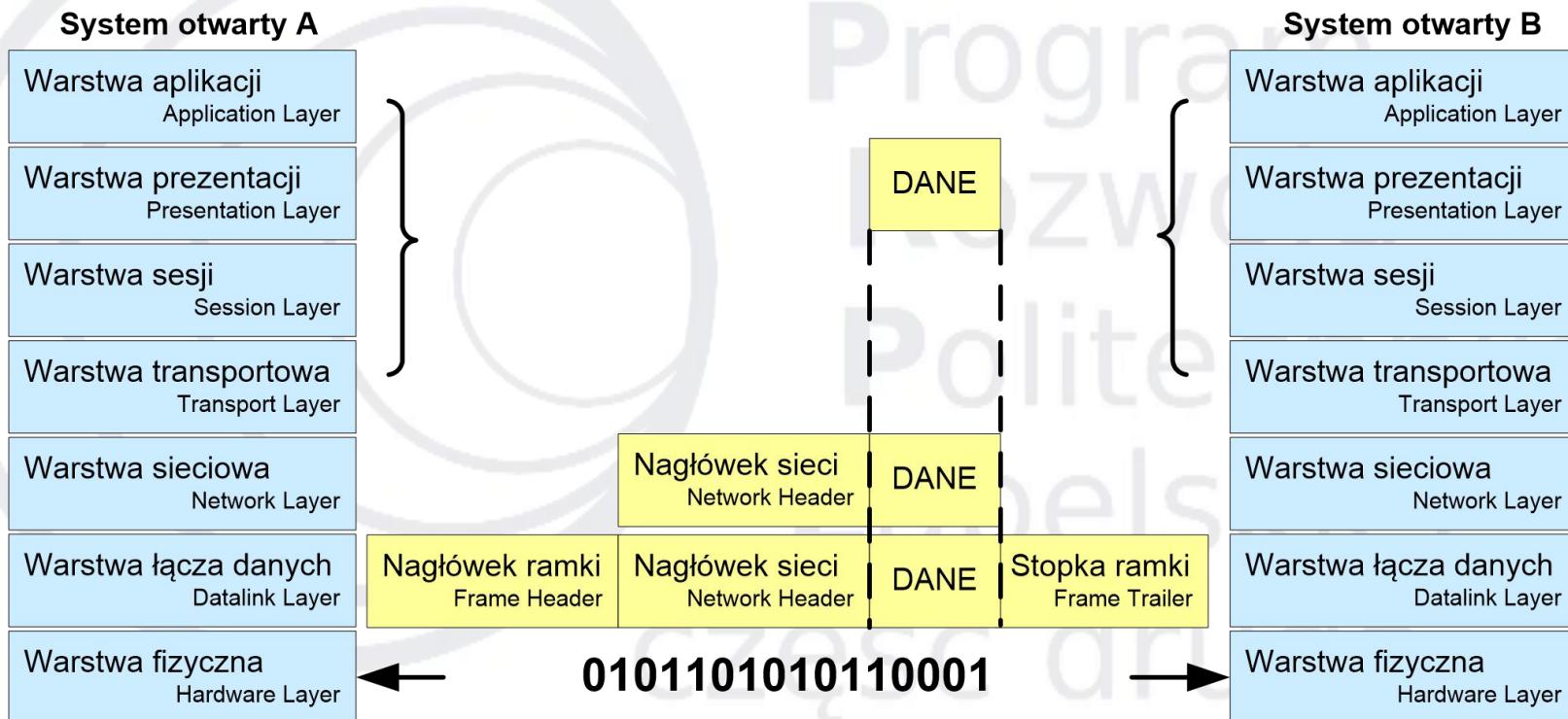
# Modele warstwowe w literaturze

RFC 1122, Internet STD 3 (1989)	Cisco Academy	Kurose, Forouzan	Comer, Kozierok	Stallings	Tanenbaum	Arpanet Ref. Model ( <a href="#">RFC 871</a> )	OSI model
4	4	5	4+1	5	5	3	7
"Internet model"	"Internet model"	"TCP/IP protocol suite"	"TCP/IP 5- layer reference model"	"TCP/IP model"	"TCP/IP 5- layer reference model"	"Arpanet reference model"	OSI model
Application	Application	Application	Application	Application	Application	Application/ Process	Application
Transport	Transport	Transport	Transport	Host-to-host or transport	Transport	Host-to-host	Transport
Internet	Internetwork	Network	Internet	Internet	Internet		Network
Link	Network interface	Data link	Data link (Network if)	Network access	Data link	Network interface	Data link
		Physical	(Hardware)	Physical	Physical		Data link

# Model warstwowy ISO-OSI

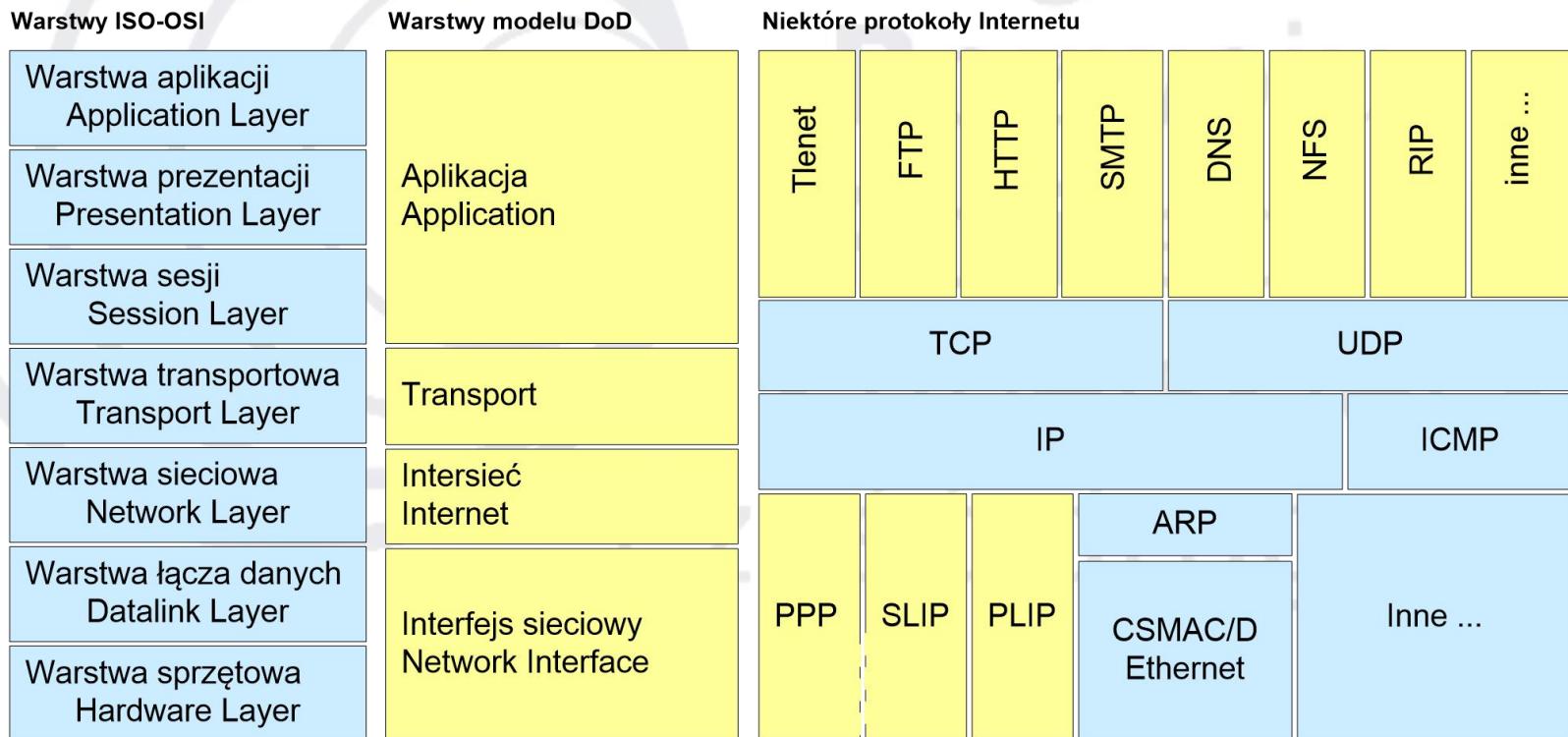


# Zastosowanie nagłówków warstwowych



# Model OSI a Internet

- W Internecie (którego powstanie poprzedziło specyfikację ISO-OSI) przyjęto uproszczony model sieci



# Wybrane urządzenia sieci teleinformatycznych L1



- **HUB – koncentrator/wzmacniak**, pozwalał na łączenie wielu urządzeń do wspólnej domeny kolizyjnej; warstwa L1 => powiela sygnały na wszystkie porty



# Wybrane urządzenia sieci teleinformatycznych L1+L2



- **NIC (Network Interface Card)** – *interfejs sieciowy*, służy do przekształcania pakietów danych w sygnały, które są przesyłane w sieci komputerowej;
  - uważane za urządzenia warstwy drugiej, ponieważ każda karta NIC przenosi unikatowy kod, nazywany adresem MAC (*Media Access Control*). Adres ten jest używany do kontrolowania komunikacji danych wobec hosta należącego do sieci
  - karty NIC pracują w określonym standardzie, np. **Ethernet**, **Token Ring**, **FDDI**, **ArcNet** czy **100VGAnylan** (wyjątek: OSA-2 ETR), i podobnie jak switche, są elementami aktywnymi sieci
  - Typy interfejsów, kart sieciowych obejmują: PCI, PCMCIA, ExpressCard, USB i PCI-Express
- **MODEM - modem kablowy** jest rodzajem mostu sieciowego, który zapewnia dwukierunkową transmisję danych za pośrednictwem łączy przewodowych lub kanałów radiowych, używane do dostępu od Internetu przez ACS

# Wybrane urządzenia sieci teleinformatycznych L2



- **BRIDGE – *most sieciowy***, urządzenie łączące segmenty sieci dokonujące filtrowania ruchu sieciowego. Sieci podłączone do mostu mogą korzystać z różnych fizycznych i logicznych protokołów łącza, W trakcie pracy analizuje tworzoną tablicę przekazywania (ang. *Forwarding DataBase*, FDB), zawierającą numery portów, do których przyłączone są urządzenia oraz adresy sprzętowe MAC.
- **SWITCH – *przełącznik sieciowy***, urządzenie łączące segmenty sieci komputerowej pracujące głównie w L2 modelu ISO/OSI; jego zadaniem jest przekazywanie ramki między segmentami sieci z doborem portu przełącznika, na który jest przekazywana; Przełączniki zarządzalne umożliwiają również wydzielanie wirtualnych sieci lokalnych (VLAN).

# Wybrane urządzenia sieci teleinformatycznych L2

- podział logiczny segmenty sieci, w oparciu o adres z ramki warstwy łącza danych



# Wybrane urządzenia sieci teleinformatycznych L3



- **ROUTER** – trasownik - urządzenie sieciowe L3, służy do łączenia różnych sieci komputerowych, pełniąc rolę węzła komunikacyjnego. Informacje zawarte w pakietach TCP/IP umożliwiają mu przekazać pakiety z dołączonej do siebie sieci źródłowej do docelowej, rozróżniając ją spośród wielu dołączonych do siebie sieci. Proces kierowania ruchem nosi nazwę trasowania, routingu lub routowania
- **L3 SWITCH** – przełącznik warstwy trzeciej, funkcjonuje w warstwie sieciowej i umożliwia przełączanie standardowe L2, wieloportowość, sieci wirtualne VLAN czy pipeline danych. Pozwalają też na podstawowe funkcje routingu pomiędzy sieciami wirtualnymi VLAN

# Wybrane urządzenia sieci teleinformatycznych L3

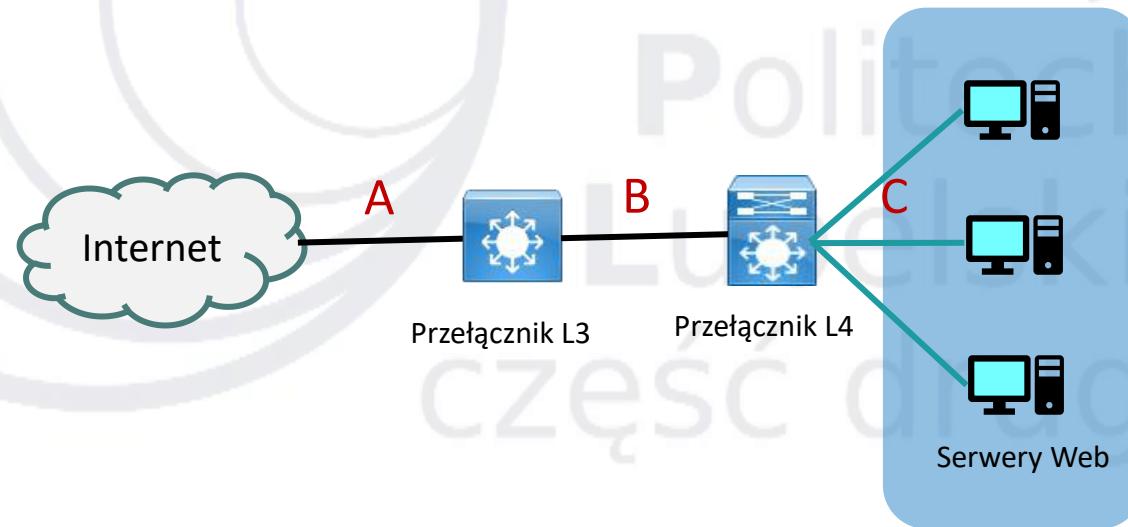
- łączenie sieci zbudowanych w oparciu o różne standardy
- odczyt danych o pakiecie oraz miejscu przeznaczenia i przekazywanie pakietu pod właściwy adres



# Wybrane urządzenia sieci teleinformatycznych L4



- **SWITCH L4** – przełącznik warstwy czwartej, poza przełączaniem L3 dodatkowo uwzględnia rodzaj ruchu sieciowego przez odczytywanie numerów portów TCP/UDP w celu podjęcia decyzji o routingu, pozwala na priorytetyzację ruchu (QoS)



# Wybrane urządzenia sieci teleinformatycznych Ln



- **MULTILAYER SWITCH (MLS)** – przełącznik wielowarstwowy, stanowi kombinację L4-7, używany do rozkładania ruchu (ang. *load balancing*), pochodzącego od aplikacji wykorzystującej TCP/IP; często z zastosowaniem translacji adresów NAT; niektóre cechują się obsługą operacji kryptograficznych

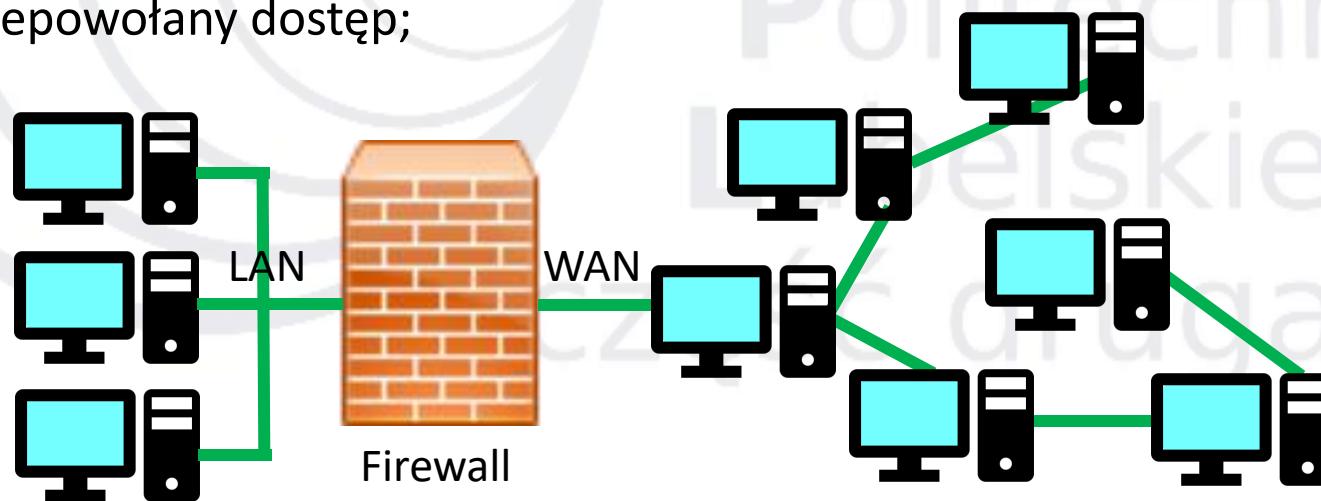


- **GATEWAY** - maszyna zapewnia interoperacyjność między sieciami, zawierająca urządzenia, takie jak translatory protokołów, konwertery szybkości, izolatory uszkodzeń lub translatory sygnałów; mogą wykonywać konwersje protokołów w celu łączenia sieci z różnymi technologiami protokołów sieciowych; w sieciach korporacyjnych brama sieciowa zwykle działa również jako serwer proxy i zapora ogniowa

# Wybrane urządzenia sieci teleinformatycznych Ln



- **FIREWALL** - jeden ze sposobów zabezpieczania sieci i systemów przed intruzami w formie systemu lub grupy systemów zarządzających dostępem pomiędzy dwiema lub więcej sieciami; Może dotyczyć sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp;



**POLITECHNIKA LUBELSKA**

**WYDZIAŁ ELEKTROTECHNIKI I INFORMATYKI**

**INFORMATYKA**



Zintegrowany  
Program  
Rozwoju  
Politechniki  
Lubelskiej -  
część druga

## Podstawy Sieci Komputerowych

## Adresacja urządzeń sieciowych warstwy L2 i L3

dr hab. inż. Konrad Gromaszek



**Fundusze  
Europejskie**  
Wiedza Edukacja Rozwój



**Rzeczpospolita  
Polska**

**Unia Europejska**  
Europejski Fundusz Społeczny



# Rodzaje komunikacji

## Komunikacja z *komutacją połączeń*

- Strony nawiązują połączenie, dla którego rezerwowane są zasoby na wszystkich stacjach pośredniczących na czas trwania połączenia  
(Przykłady zastosowań: telefonia, radiofonia, telewizja)

## Komunikacja z *komutacją pakietów*

- Strony wysyłają dane w formie niezależnie przesyłanych pakietów, kiedy uznają to za stosowne. Po przesłaniu pakietu, wszystkie zasoby są zwalniane  
(Przykład: większość klasycznych sieci LAN)

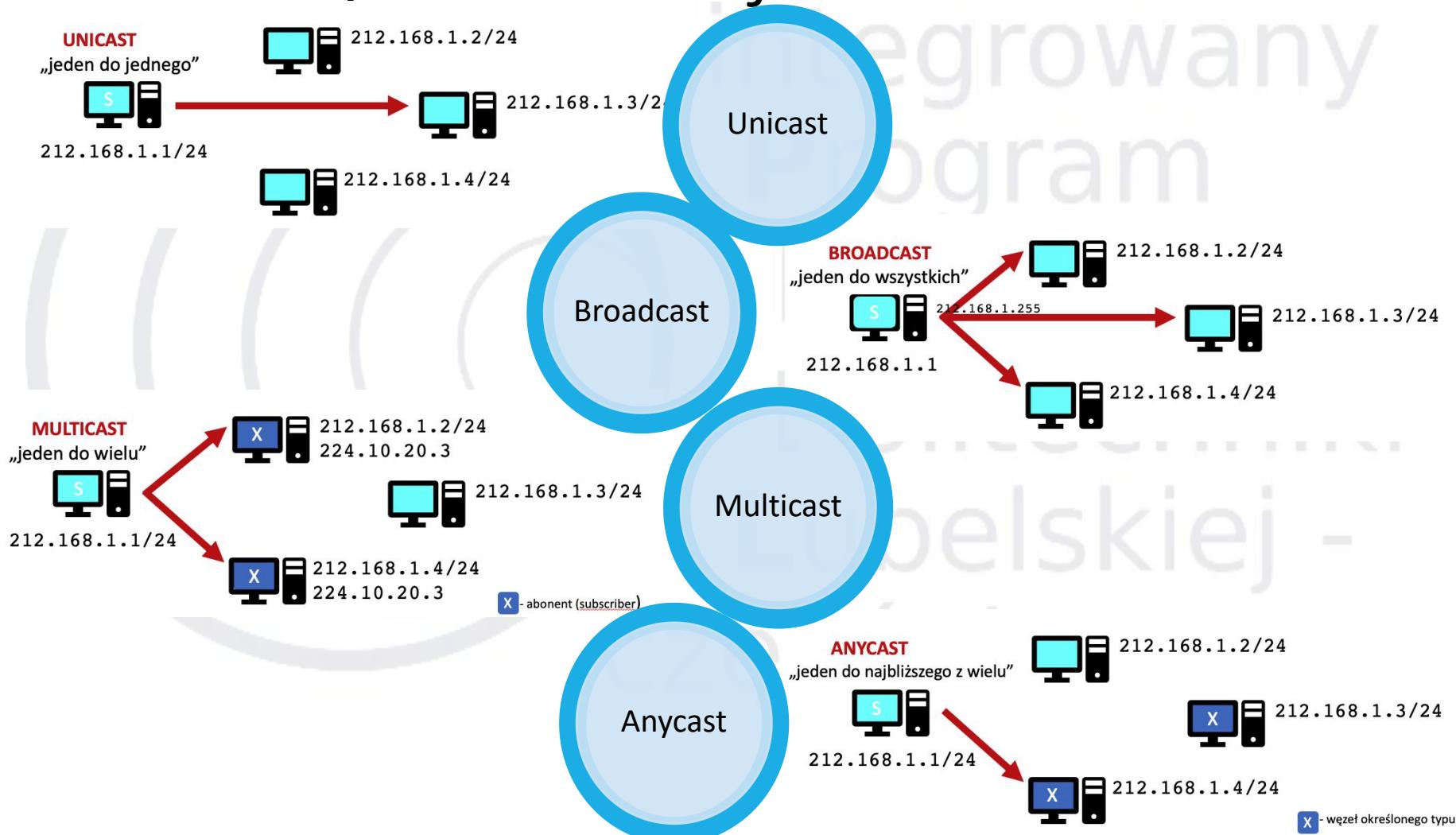
## Metody pośrednie

- Metody, które próbują łączyć cechy obu powyższych podejść  
(Przykład: ISDN)

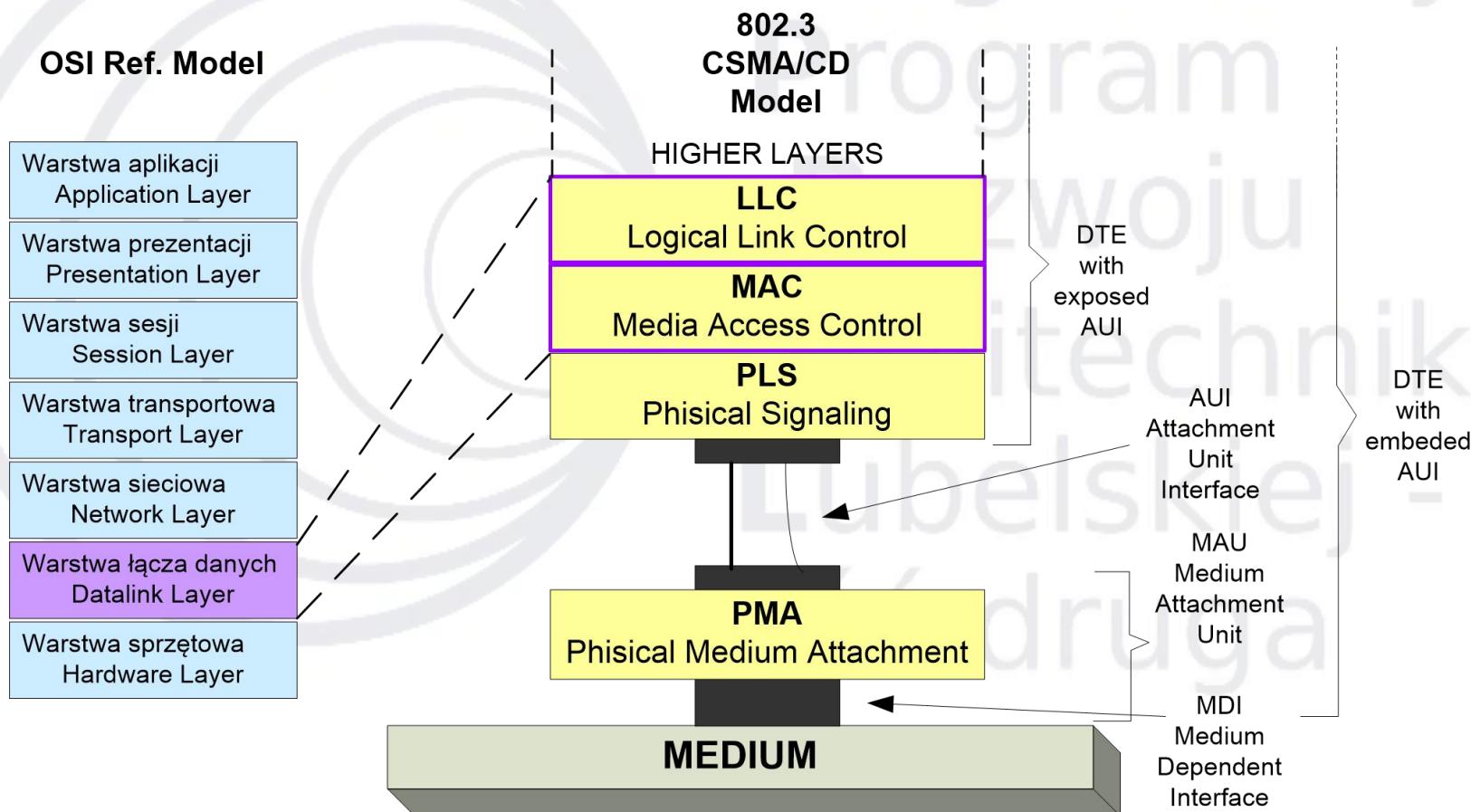
# Rodzaje adresacji w sieciach pakietowych

- Adresowanie płaskie:
  - Przy nadawaniu adresu jednostka zwykle otrzymuje kolejny wolny
  - Brak hierarchii w schemacie adresowania, np. adres MAC
- Adresowanie hierarchiczne:
  - Nie można przydzielać adresów losowo
  - Przy nadawaniu adresu ważne jest położenie jednostki w strukturze. Na przykład adres IP
- Adresowanie w warstwie sieciowej jest niezależne od „płaskiego” adresowania w warstwie DLC (adres = adres sieci + adres stacji)

# Rodzaje transmisji

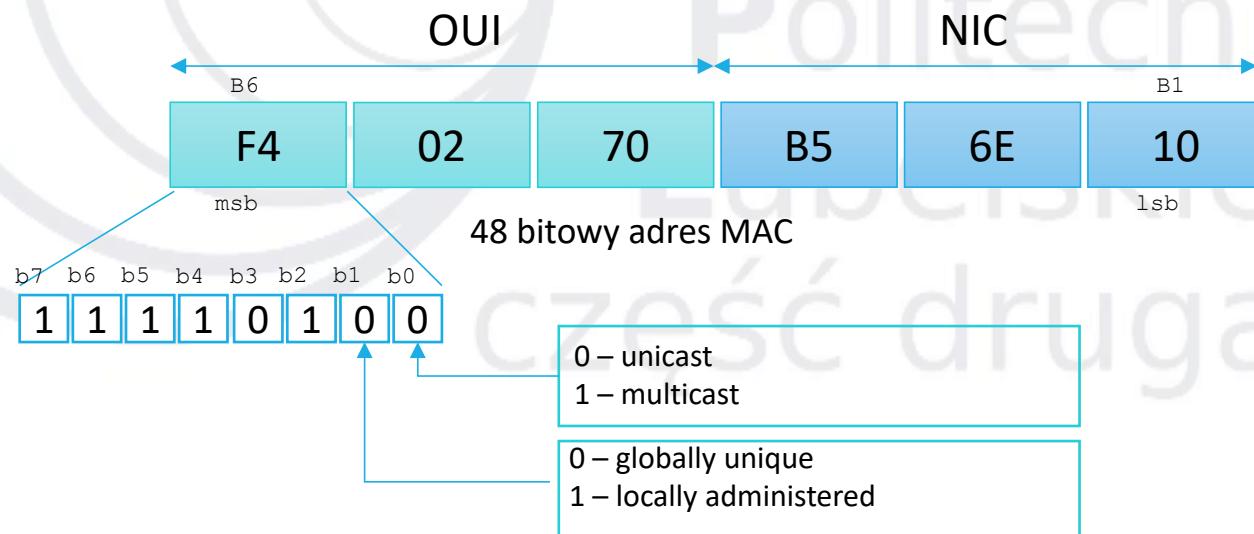


# Media Access Control



# Adres MAC

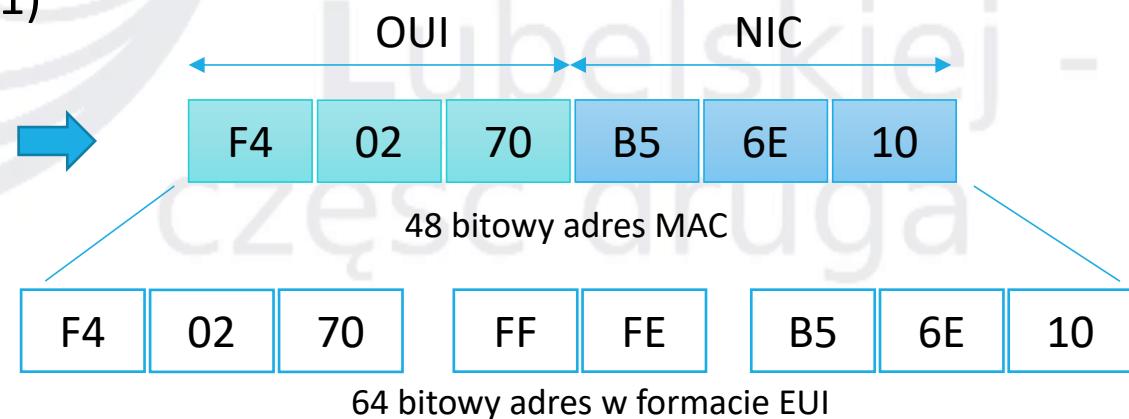
- adres **MAC** (ang. **MAC address**) jest 48-bitową liczbą zapisywaną heksadecymalnie (szesnastkowo); pierwsze 24 bity liczby oznaczają producenta karty sieciowej (ang. vendor code), lub *Organizationally Unique Identifier* (OUI) pozostałe 24 bity są unikatowym identyfikatorem danego egzemplarza karty (NIC)



# Adres MAC

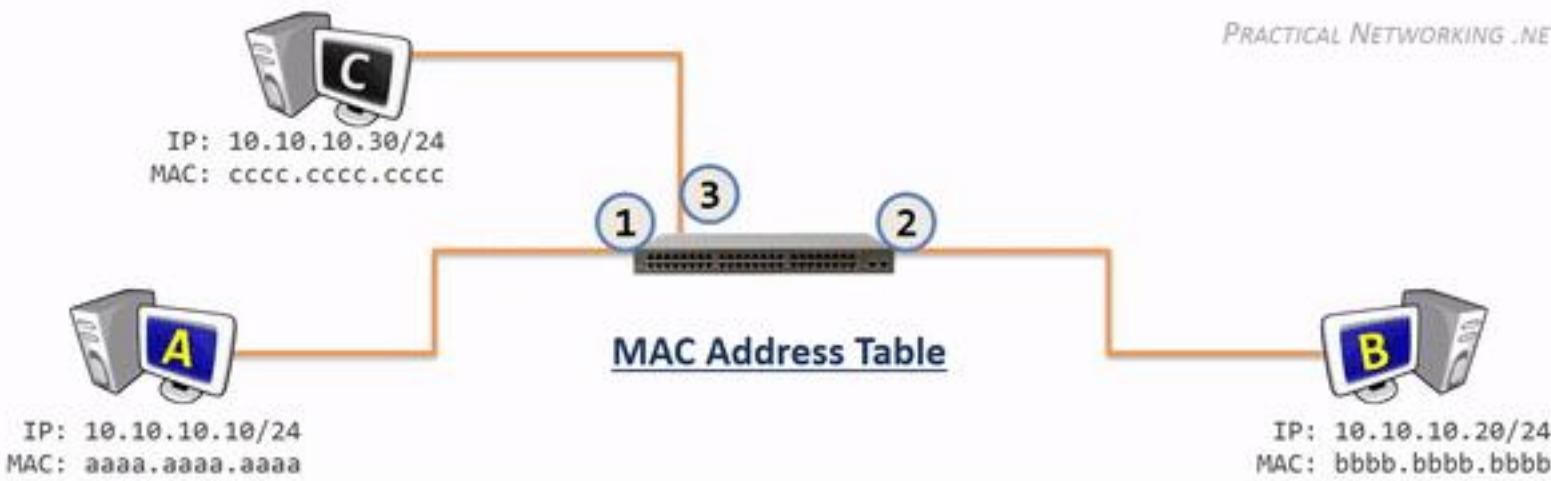
- adresy prefiksów, przydzielonych producentom urządzeń sieciowych dostępne są na <http://standards-oui.ieee.org/oui/oui.txt>
- istnieją również zarezerwowane adresy MAC służące chociażby sterowaniu przepływem, testom czy dla przyszłych zastosowań
- na potrzeby współczesnych zastosowań wprowadzono format EUI-64 (RFC 2373, RFC4291)

F4-02-70 (hex) Dell Inc.  
F40270 (base 16)  
Inc. One Dell  
Way Round Rock TX  
78682  
US



# Adresowanie MAC w LAN

- Przełącznik sieciowy L2
  - Uczenie (**Learning**) => tabela odwzorowania portów na adresy MAC podłączonych urządzeń
  - Zalewanie (**Flooding**)
  - Przekazywanie (**Forwarding**)
- Ograniczenie: pojedynczy segment sieci!



Źródło rysunku: <https://www.practicalnetworking.net/wp-content/uploads/2016/01/packtrav-host-switch-host.gif>

# Adresowanie w warstwie sieci

- Warstwa sieciowa odgrywa b. ważną rolę w sieciach składających się z podsieci
- Rola adresacji w funkcjonowaniu protokołów warstwy sieciowej
  - Pozwala na dostarczenie pakietów (datagramów) od źródła do celu (rutowanie)
  - Pakiet (datagram) posiada wszystkie informacje pozwalające na rutowanie i rozpoznawanie przez odbiorców (analogia urzędu pocztowego)
  - Zapewnienie komunikacji pomiędzy hostami znajdującymi się w tej samej lub różnych sieciach
  - Hierarchiczny sposób adresowania pakietów w IPv4

# Struktura adresu IPv4

- Adres IP w notacji kropkowo-dziesiętnej

192	.	168	.	100	.	1
11000000	10101000	01100100	00000001			

- 32 bitowy adres IPv4

192	.	168	.	100	.	1
11000000	10101000	01100100	00000001			

- Oktet

192	.	168	.	100	.	1
11000000	10101000	01100100	00000001			

- Sieć

192	.	168	.	100	.	1
11000000	10101000	01100100	00000001			

- Host

# System numeryczny - zasady

1. Wszystkie cyfry zaczynają się od 0
2. Podstawa systemu liczbowego posiada  $n$  cyfr:
  - s. dziesiętny:  $n_{10} = 10$  cyfr (0-9)
  - s. binarny:  $n_2 = 2$  cyfry (0, 1)
  - s. szesnastkowy:  $n_{16} = 16$  cyfr (0-9,A-F)
- Wielokrotności odpowiednich podstaw:
  - Podstawa 10:    10000        1000        100        10        1
  - Podstawa 2:        16              8              4              2        1
  - Podstawa 16:     65536        4096        256        16        1

# Dziesiętny system liczbowy

Cyfry (10) : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

	$10^4$	$10^3$	$10^2$	$10^1$	$10^0$
	<u>10,000</u>	<u>1,000</u>	100	10	1
1309		1	3	0	9
99				9	9
100			1	0	0

# Dziesiętny system liczbowy

- W **systemie dziesiętnym** liczba taka może przyjmować wartość w zakresie od 0 do 255
- W stosowanym zapisie pozycyjnym miejsce które reprezentuje cyfra 2 odpowiada liczbie, tzw. wartości bazy ( $n_{10}=10$ ) podniesiona do potęgi drugiej
- Dla liczby dziesiętnej 245, wartość 2 reprezentuje liczbę  $2 \cdot 10^2$  (2 razy 10 do potęgi 2)

$$245 = (2 \cdot 10^2) + (4 \cdot 10^1) + (5 \cdot 10^0)$$

	$10^4$	$10^3$	$10^2$	$10^1$	$10^0$
10000					
245			2	4	5

# Dwójkowy system liczbowy

- W ***dwójkowym systemie liczbowym*** podstawą jest liczba 2, posiada tylko dwie cyfry
- Oznacza ro, że każda następna pozycja reprezentuje wzrost wartości o kolejną potęgę liczby 2
- Ograniczając się do 8 bitów, kolejne pozycje będą reprezentować następujące wartości

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1

# Dwójkowy system liczbowy

- System pozycyjny o podstawie 2, posiada tylko dwie cyfry
- Podczas interpretowania bajtu jako liczbę dziesiętną, do obliczanej sumy wejdą tylko potęgi liczby 2, związane z pozycjami, na których znajduje się cyfra
- Pozycje, na których znajduje się cyfra 0, mają wartość zero, przez co nie wpływają na całkowitą wartość przeliczanej liczby

$$\mathbf{11111111 = 128+64+32+16+8+4+2+1 = 255}$$

- Występowanie cyfry 1 na każdej pozycji oznacza, że wartość liczby po przeliczeniu jest sumą wartości określonych dla wszystkich pozycji

# Dwójkowy system liczbowy

Cyfry (2) : 0, 1

Liczba:

	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
	128	64	32	16	8	4	2	1
2							1	0
10					1	0	1	0
17				1	0	0	0	1
255	1	1	1	1	1	1	1	1

# Konwersja liczb z systemu binarnego na dziesiętny

Postać wykładnicza

Pozycja

Bity

Sumowanie liczb

Wartość dziesiętna

$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1
1	1	1	0	1	1	0	1
1 Bajt / 1 oktet							
$128 + 64 + 32 + 0 + 8 + 4 + 0 + 1$							
237							

11101101 w systemie binarnym = liczba 245 w systemie dziesiętnym

# Konwersja adresów IPv4 z postaci binarnej na postać kropkowo-dziesiętną

1

2

3

10101100000100000000101000011001

10101100

00010000

00001010

00011001

1	x 128	128
0	x 64	0
1	x 32	32
0	x 16	0
1	x 8	8
1	x 4	4
0	x 2	0
0	x 1	0

0	x 128	0
0	x 64	0
0	x 32	0
1	x 16	16
0	x 8	0
0	x 4	0
0	x 2	0
0	x 1	0

0	x 128	0
0	x 64	0
0	x 32	0
0	x 16	0
1	x 8	8
0	x 4	0
1	x 2	2
0	x 1	0

0	x 128	0
0	x 64	0
0	x 32	0
1	x 16	16
1	x 8	8
0	x 4	0
0	x 2	0
1	x 1	1

172

16

10

25

172.16.10.25

# Konwersja liczb z systemu dziesiętnego na system binarny

172 Liczba **172** jest większa od 128, wstawić **1** na pozycji odpowiadającej 128  
— 128 i odjąć 128

— 44 jest mniejsze od 64, wstawić **0** na pozycji odpowiadającej 64

— 0

— 44 jest większe niż 32, wstawić **1** na pozycji odpowiadającej 32  
— 32 i odjąć 32

— 12 jest mniejsze niż 16, wstawić **0** na pozycji odpowiadającej 16

— 0

— 12 jest większe niż 8, wstawić **1** na pozycji odpowiadającej 8  
— 8 i odjąć 8

— 4 jest równe 4, wstawić **1** na pozycji odpowiadającej 4  
— 4 i odjąć 32

— 0 jest mniejsze niż 2, wstawić **0** na pozycji odpowiadającej 2

— 0

— 0 jest mniejsze niż 1, wstawić **0** na pozycji odpowiadającej 0

— 0 Zrobione, odpowiedź:  $172 = \boxed{10101100}$

**172.16.10.25**

**10101100**

# Konwersja liczb z systemu dziesiętnego na system binarny

25 Liczba **25** jest mniejsza od 128, wstawić **0** na pozycji odpowiadającej 128

0

25 jest mniejsze od 64, wstawić **0** na pozycji odpowiadającej 64

0

25 jest mniejsze od 32, wstawić **0** na pozycji odpowiadającej 32

0

25 jest większe od 16, wstawić **1** na pozycji odpowiadającej 16

16

9 jest większe od 8, wstawić **1** na pozycji odpowiadającej 8

8

1 jest mniejsze niż 4, wstawić **0** na pozycji odpowiadającej 4

0

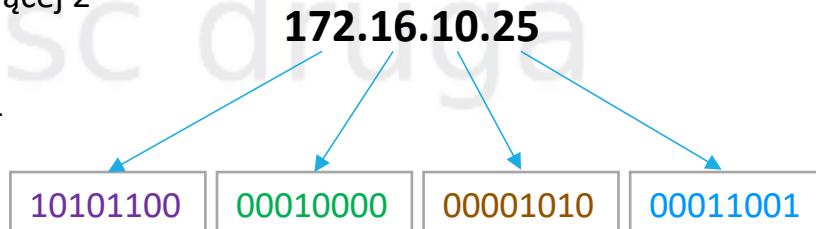
1 jest mniejsze niż 2, wstawić **0** na pozycji odpowiadającej 2

1

0 jest równe 1, wstawić **1** na pozycji odpowiadającej 1

0

0 Zrobione, odpowiedź:  $25 = \text{00011001}$



# Konwersja adresów IPv4 z postaci binarnej na postać kropkowo-dziesiętną

Postać kropkowo-dziesiętna adresu IPv4 **172.16.10.25**

Rozdzielić liczby dziesiętne i konwertować każdą z nich z osobna

Konwersja liczby **172**

$172-128=44$	$\rightarrow$	1	$\times 128$
44	$\rightarrow$	0	$\times 64$
$44-32=12$	$\rightarrow$	1	$\times 32$
12	$\rightarrow$	0	$\times 16$
$12-8=4$	$\rightarrow$	1	$\times 8$
$4-4=0$	$\rightarrow$	1	$\times 4$
0	$\rightarrow$	0	$\times 2$
0	$\rightarrow$	0	$\times 1$

**10101100**

Konwersja liczby **16**

16	$\rightarrow$	0	$\times 128$
16	$\rightarrow$	0	$\times 64$
16	$\rightarrow$	0	$\times 32$
$16-16=0$	$\rightarrow$	1	$\times 16$
0	$\rightarrow$	0	$\times 8$
0	$\rightarrow$	0	$\times 4$
0	$\rightarrow$	0	$\times 2$
0	$\rightarrow$	0	$\times 1$

**00010000**

Konwersja liczby **10**

10	$\rightarrow$	0	$\times 128$
10	$\rightarrow$	0	$\times 64$
10	$\rightarrow$	0	$\times 32$
10	$\rightarrow$	0	$\times 16$
$10-8=2$	$\rightarrow$	1	$\times 8$
2	$\rightarrow$	0	$\times 4$
$2-2=0$	$\rightarrow$	1	$\times 2$
0	$\rightarrow$	0	$\times 1$

**00001010**

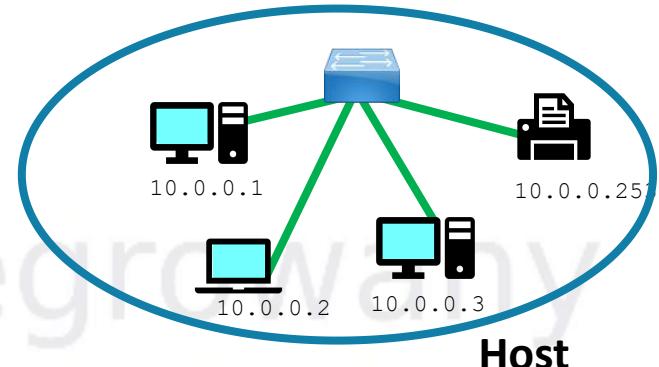
Konwersja liczby **25**

25	$\rightarrow$	0	$\times 128$
25	$\rightarrow$	0	$\times 64$
25	$\rightarrow$	0	$\times 32$
$25-16=9$	$\rightarrow$	1	$\times 16$
$9-8=1$	$\rightarrow$	1	$\times 8$
1	$\rightarrow$	0	$\times 4$
1	$\rightarrow$	0	$\times 2$
$1-1=0$	$\rightarrow$	1	$\times 1$

**00011001**

Binarna postać adresu IPv4: **1010110000100000000101000011001**

# Rodzaje adresów



	Network	Host	
<b>Network address (Adres sieci)</b>	10 0 0 0	0 0 0 0	0
	00001010 00000000 00000000 00000000		
<b>Broadcast address (Adres rozgłoszeniowy)</b>	10 0 0 0	255	0 0 0 1
	00001010 00000000 00000000 11111111		
<b>Host address (Adres hosta)</b>	10 0 0 0	1	0 0 0 1
	00001010 00000000 00000000 00000001		
<b>Subnet mask (Maska podsieci)</b>	<b>255.255.255.0</b>		

# Podział na część sieciową i hosta

- 32b **Maska sieci** określa podział na część sieciową (1) i część hosta (0)



**Network mask**  
Maska sieciowa

11111111 . 11111111 . 11111111 . 00000000

**Dotted decimal**  
Notacja kropkowo-dziesiętna

255 . 255 . 255 . 0

**Slash notation**  
Notacja CIDR

/24

- Przykład działania

- Adres sieci 172.168.0.0
- Maska sieci 255.255.0.0
- Notacja CIDR /16

10101100.10101000|00000000.00000000  
11111111.11111111|00000000.00000000

# Znaczenie maski sieciowej

## Maska podsieci

/8 lub 255.0.0.0

/16 lub 255.255.0.0

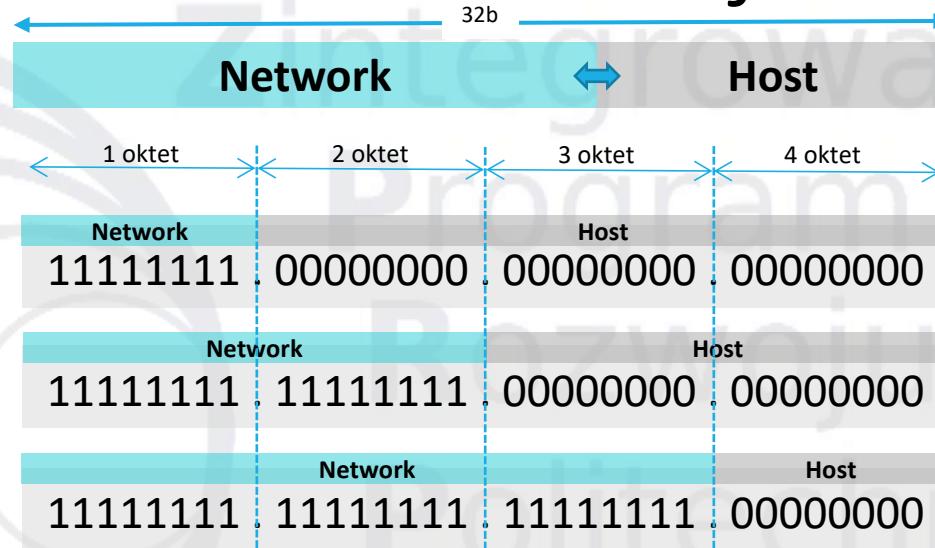
/24 lub 255.255.255.0

- Liczba bitów części hostowej określa liczbę hostów

- Przykład działania

- Adres sieci 172.168.0.0
- Maska sieci 255.255.0.0
- Notacja CIDR /16

10101100.10101000.00000000.00000000  
11111111.11111111.00000000.00000000

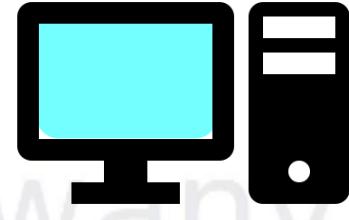


# Maska podsieci a adres rozgłoszeniowy

Adres sieci		Maska sieci	Adres rozgłoszeniowy
10.16.0.0	/16	<b>255.255.0.0</b>	10.16. <b>255.255</b>
192.168.1.0	/24	<b>255.255.255.0</b>	192.168.1. <b>255</b>
172.0.0.0	/8	<b>255.0.0.0</b>	172. <b>255.255.255</b>
192.168.0.0	/16	<b>255.255.0.0</b>	192.168. <b>255.255</b>
10.16.0.0	/16	<b>255.255.0.0</b>	10.16. <b>255.255</b>
172.0.0.0	/24	<b>255.255.255.0</b>	172.0.0. <b>255</b>
10.2.1.0	/24	<b>255.255.255.0</b>	10.2.1. <b>255</b>

- Wszystkie 1 w części hostowej adresu

# Adres IP hosta



212.168.1.2/24

- Adres hosta zawiera:

- Część sieciową adresu
- Unikalną kombinację 0 i 1 w części hostowej adresu
  - Nie mogą być same 0 (network address)
  - Nie mogą być same 1 (broadcast address)
- Maskę podsieci do określenia części sieciowej

- Adresy prywatne

- RFC 1918

10.0.0.0 - 10.255.255.255 (10.0.0.0 /8)

172.16.0.0 - 172.31.255.255 (172.16.0.0 /12)

192.168.0.0 - 192.168.255.255 (192.168.0.0 /16)

- Te adresy nie mogą być rutowane przez Internet
- Zastosować NAT/PAT
- Powinien być blokowany przez ISP

# Adresy specjalne unicast

- Loopback Address
  - 127.0.0.0 to 127.255.255.255
- Link-Local Addresses
  - 169.254.0.0 to 169.254.255.255 (169.254.0.0 /16)
  - Otrzymywany automatycznie gdy nie odpowiada serwer DHCP

# Zakres hostów

	<b>Adres sieci</b>	<b>Maska sieci</b>	<b>Adres rozgłoszeniowy</b>
	10.16.0.0	<b>255.255.0.0</b>	10.16.255.255
<b>zakres hostów</b>	<b>10.16.0.1</b>	<b>← /16 →</b>	<b>10.16.255.254</b>
	192.168.1.0	<b>255.255.255.0</b>	192.168.1.255
<b>zakres hostów</b>	<b>192.168.1.1</b>	<b>← /24 →</b>	<b>192.168.1.254</b>
	172.0.0.0	<b>255.0.0.0</b>	172.255.255.255
<b>zakres hostów</b>	<b>172.0.0.1</b>	<b>← /8 →</b>	<b>172.255.255.254</b>
	192.168.0.0	<b>255.255.0.0</b>	192.168.255.255
<b>zakres hostów</b>	<b>192.168.0.1</b>	<b>← /16 →</b>	<b>192.168.255.254</b>

# Zakres hostów binarnie

192.168.1.0	(net)	11000000.10101000.00000001.00000000
255.255.255.0	(sm)	11111111.11111111.11111111.00000000
192.168.1. <b>1</b>		11000000.10101000.00000001. <b>00000001</b>
192.168.1. <b>254</b>		11000000.10101000.00000001. <b>11111110</b>
192.168.1.255	(bcst)	11000000.10101000.00000001.11111111

10.2.0.0	(net)	00001010.00000010.00000000.00000000
255.255.0.0	(sm)	11111111.11111111.00000000.00000000
10.2.0. <b>1</b>		00001010.00000010. <b>00000000.00000001</b>
10.2. <b>255.254</b>		00001010.00000010. <b>11111111.11111110</b>
10.2.255.255	(bcst)	00001010.00000010.11111111.11111111

# Maska podsieci

- Maska podsieci nie zawsze kończy się w granicach oktetów!

192.168.16.0	(net)	11000000.10101000.00010000.00000000
255.255.240.0	(sm)	11111111.11111111.11110000.00000000
192.168.16.1		11000000.10101000.00010000.00000001
192.168.31.254		11000000.10101000.00011111.11111110
192.168.31.255	(bcst)	11000000.10101000.00011111.11111111

- Stąd: liczba hostów:  $2^{12} - 2 = 4096 - 2 = \underline{4094}$

# Obliczanie liczby potrzebnych podsieci / komputerów

- Dana jest sieć 212.168.1.0 /24. Wyznaczyć tak dużo podsieci, jak to jest możliwe, 60 komputerów na podsieć

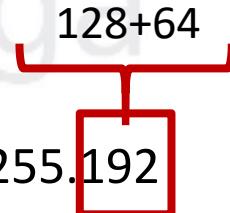
$2^{10}$	$2^9$	$2^8$	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
1024	512	256	128	64	32	16	8	4	2	1

Liczba pożyczonych bitów

10	9	8	7	6	5	4	3	2	1	-
1024	512	256	128	64	32	16	8	4	2	

Liczba hostów lub podsieci

- 212.168.1.0 => 212.168.001. 00000000
- /24 => 255.255.255. **11000000** => 255.255.255.192



# Obliczanie liczby potrzebnych podsieci / komputerów

- Dana jest sieć 212.168.1.0 /24. Wyznaczyć tak dużo podsieci, jak to jest możliwe, 60 komputerów na podsieć
- 
- $212.168.1.0 \Rightarrow \mathbf{212.168.001.0000000}$
- $/24 \Rightarrow \mathbf{255.255.255.11000000} \Rightarrow 255.255.255.192$
- Nowa maska podsieci: 255.255.255.192 (/26)
- Liczba komputerów na podsieć: 6 bitów,  $64 - 2 = \mathbf{62}$
- Liczba podsieci: **4** (bo 2 bity : {00, 01, 10, 11})



## Podstawy Sieci Komputerowych

### Rodzina standardów IEEE 802.1 i IEEE 802.3

Warstwa fizyczna. Media transmisyjne.  
Systemy okablowania strukturalnego

dr hab. inż. Konrad Gromaszek



**Fundusze  
Europejskie**  
Wiedza Edukacja Rozwój



**Rzeczpospolita  
Polska**

**Unia Europejska**  
Europejski Fundusz Społeczny

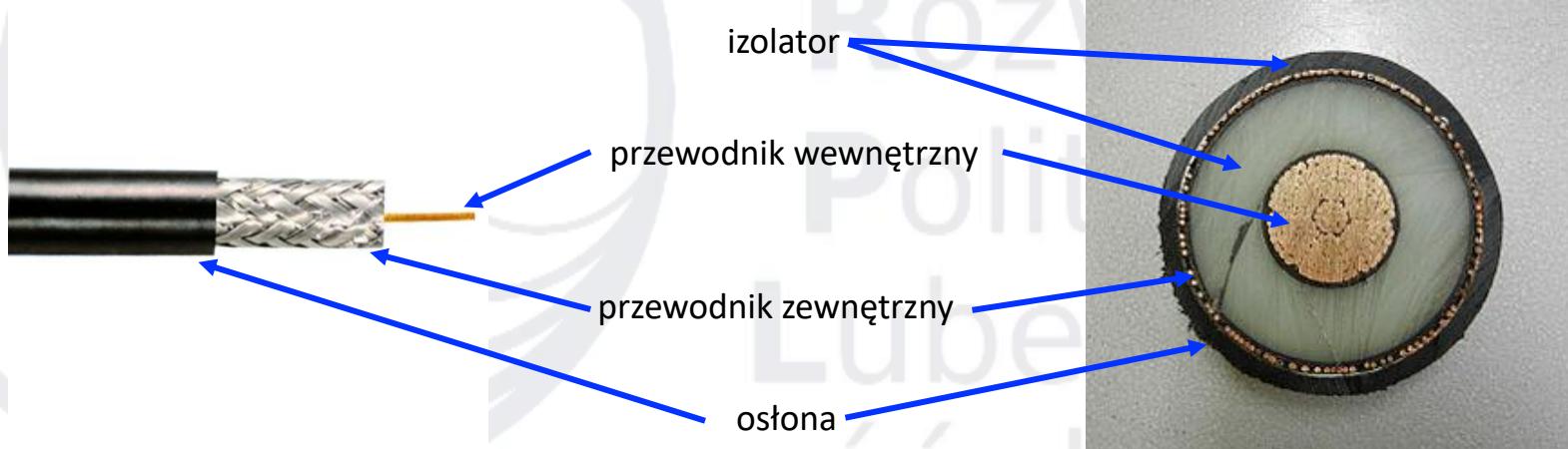


# Funkcje warstwy fizycznej

- Warstwa fizyczna przesyła i odbiera sygnały zaadresowane dla wszystkich protokołów jej stosu oraz aplikacji, które je wykorzystują
- Wysyłanie strumieni danych:
  - zamieniać dane znajdujące się w ramkach na strumienie binarne
  - realizować oczekiwany przez warstwę łącza danych metodę dostępu do medium komunikacyjnego
  - przesyłać ramki danych szeregowo w postaci strumieni binarnych
- Odbieranie strumieni danych:
  - oczekiwanie na zaadresowane do hosta transmisje przychodzące
  - odbiór odpowiednio zaadresowanych strumieni
  - przesyłanie binarnych strumieni do warstwy łącza danych w celu złożenia ich z powrotem w ramki

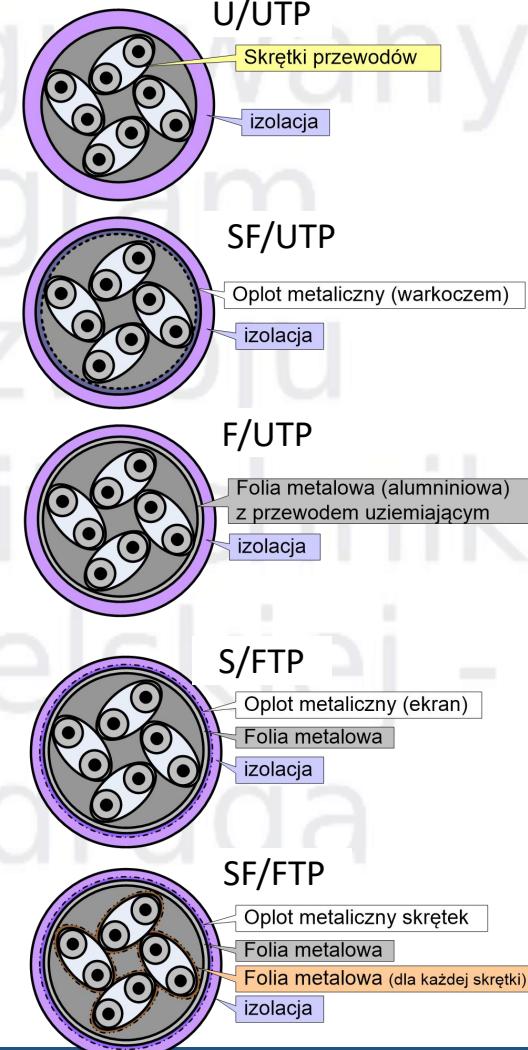
# Media komunikacyjne – coax

- **Kabel koncentryczny** (ang. *coaxial cable*) - zbudowany jest z litego izolowanego przewodu miedzianego, przewodu ekranującego- uziemiającego oraz z zewnętrznej warstwy ochronnej



# Media komunikacyjne - skrętka

- Sposób oznaczania określa norma ISO/IEC 11801:2002
- Rozróżnia się następujące rodzaje skrętki:
  - skrętkę nieekranowaną (U/UTP),
  - ekranowaną folią,
    - z dodatkowymi płaszczami z folii (F/UTP i U/FTP)
    - z dodatkowymi płaszczami z metalowej siatki (SF/UTP, S/FTP i SF/FTP)



# Media komunikacyjne - skrętka

- Przydatność do transmisji cyfrowych określają **kategorie**, a przydatność do aplikacji - **klasy** kabli miedzianych
- Klasy skrętki według europejskiej normy EN 50173:

...

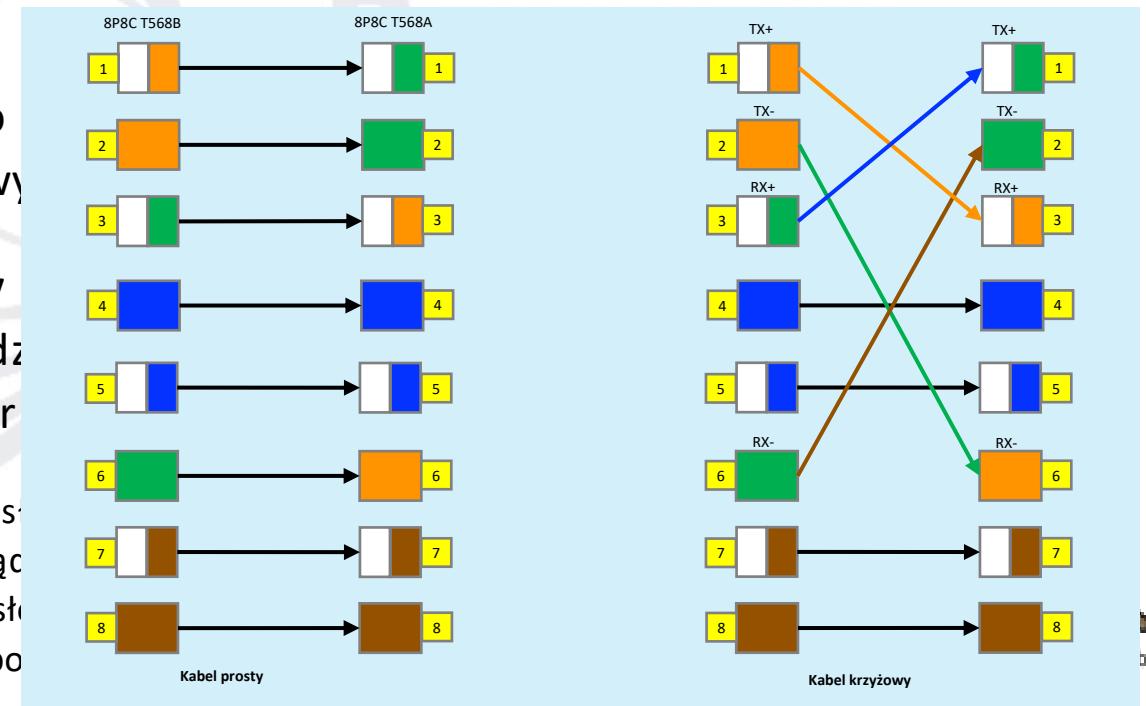
**klasa I** (kat. 8.1) – w trakcie rozwoju (opisana w *ANSI/TIA-568-C.2-1, ISO/IEC 11801 3rd Ed.*), wykorzystująca pasmo częstotliwości 1600–2000 MHz; prędkość transmisji ponad 40 Gbit/s;

**klasa II** (kat. 8.2) – w sprzedaży (opisana w *ISO/IEC 11801 3rd Ed.*), wykorzystująca pasmo częstotliwości 1600–2000 MHz.

W amerykańskiej normie **TIA/EIA 568A** dodatkowo występuje powiązana z **klasą C, kategoria 4** dla szybkich sieci lokalnych, przeznaczona dla aplikacji, wykorzystujących pasmo częstotliwości do 20 MHz

# Media komunikacyjne - skrętka

- Do typowych zastosowań sieci LAN, najczęściej stosuje się okablowanie UTP kategorii 5e ze złączem RJ-45
- Dwa rodzaje kabli
  - **Kabel prosty** – do przełącznika sieciowego
  - **Kabel krzyżowy** – do interfejsów urządzeń (host – host, router)
- Rozwój technologii przyniósł (głównie ze względu na urządzenia Ethernet, komputery przemysłowe) że potrzeby mogą pracować jak po-



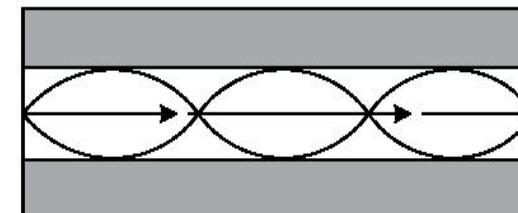
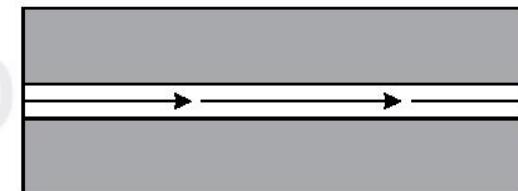
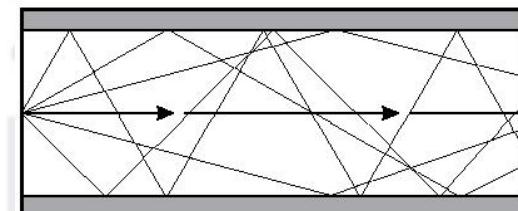
# Media komunikacyjne - światłowód

- W światłowodach do transmisji informacji wykorzystywana jest wiązka światła, która jest odpowiednikiem prądu w innych kablach miedzianych i modulowana zgodnie z treścią przekazywanych danych
- Światłowód wykonany ze szkła kwarcowego, składa się z rdzenia (złożonego z jednego lub wielu włókien), okrywającego go płaszcza oraz warstwy ochronnej



# Kabel światłowodowy

- Włókno światłowodowe jest z reguły pokryte warstwą polimeru (tzw. **pokrycie pierwotne**), zabezpieczające włókno przed wpływem otoczenia; kolejne warstwy ochronne => kabel światłowodowy
- Światłowody dzieli się na:
  - **jednomodowe** (szklane)
  - **wielomodowe**
    - **skokowe** (gł. plastikowe)
    - **gradientowe** (gł. szklane)



# Porównanie okablowania (Cu vs. SiO<sub>2</sub>)

Okablowanie miedziane	Okablowanie światłowodowe
<ul style="list-style-type: none"><li>-Długość łącza 100 m (kabel 4 parowy)</li><li>-Wrażliwość na zakłócenia EM</li><li>-Łatwy podsłuch</li><li>-Występowanie przesłuchów</li><li>-Duża masa i średnica kabla (UTP, STP)</li><li>-Oddzielne prowadzenie zasilających i kabli sygnałowych, podwójne i szerokie kanały kablowe</li><li>-Problemy z właściwym uziemianiem (STP)</li><li>-Pasmo 100 MHz (100m, kat. 5), 200 MHz (100m, kat. "6") 600 MHz (100m, kat. "7") – kilka rodzaje łączy</li></ul>	<ul style="list-style-type: none"><li>-Długość łącza kilkadziesiąt km</li><li>-Odporność na zakłócenia EM</li><li>-Możliwość instalacji z kablami energetycznymi</li><li>-Nie wytwarza pola EM (trudny do podsłuchania)</li><li>-Brak przesłuchów</li><li>-Izolacja galwaniczna</li><li>-Bardzo szerokie pasmo</li><li>-Mała masa i rozmiary - mniejsze, tańsze trakty kablowe</li></ul>

# Media bezprzewodowe

- Łącza podczerwone
  - fale elektromagnetyczne z zakresu 700-1500 nm
  - mały zasięg (kilkanaście metrów), niewielkie zaniki sygnału, wysoka tłumienność, duża wrażliwość na zakłócenia pochodzące ze źródła promieniowania widzialnego
  - brak potrzeby zezwolenia (licencji) odpowiednich agencji rządowych na ich stosowanie
- Łącza radiowe
  - stosuje częstotliwości radiowe z zakresu 1-30 GHz
  - połączenia międzybudynkowe, komunikacja w terenie otwartym, zapewnienie redundantnych połączeń dublujących połączenia kablowe
  - mobilność, sieci sensoryczne

Rozwinięcie:  
wykład o sieciach  
bezprzewodowych

# Okablowanie strukturalne<sub>(1/3)</sub>

- System Okablowania Strukturalnego (SOS) stanowi infrastrukturę kablową zainstalowaną w budynku lub kompleksie budynków, pozwalającą na korzystanie z:
  - sieci komputerowej (LAN)
  - usług telefonicznych (teleinformatycznych)
  - systemu bezpieczeństwa i monitorowania
  - systemu ochrony przeciwpożarowej i sygnalizacji
- jest to system, w którym normalizuje się topologię, elementy, parametry i sterowanie → inteligentny budynek

# Okablowanie strukturalne (3/3)

## Okablowanie strukturalne

poziome

pionowe

międzybudynkowe

- o. **poziome** – część systemu łącząca punkt abonencki z punktem dystrybucyjnym (lokalnym lub kondygnacyjnym), odległość <100m
- o. **pionowe** (ang. *backbone*) – łączy Pośrednie Punkty Dystrybucyjne (IDF) z Głównym Punktem Rozdzielczym (MDF), najczęściej układane w pionowych szybach pomiędzy kondygnacjami; długość segmentu zależy ściśle od medium: Telefoniczny UTP – 800m, Skrętka UTP/FTP – 90m, Światłowód 2000m
- o. **międzybudynkowe (kampusowe)** – ma zapewnić łączność teleinformatyczną między oddalonymi budynkami; logicznie łączy Budynkowy Punkt Dystrybucyjny z Centralnym Punktem Dystrybucyjnym

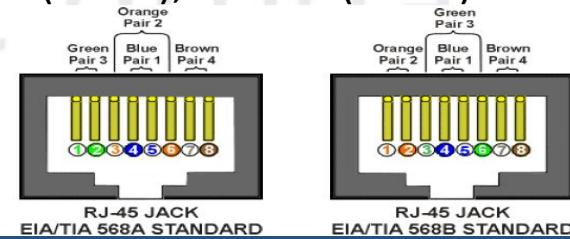
# Punkty rozdzielcze SOS

Nomenklatura polska	Nazewnictwo anglojęzyczne
<p>PCS – Punkt Centralny Sieci – zawiera farmę serwerów, punkt dostępu do Internetu i CPD, jest sercem infrastruktury informatycznej</p> <p>CPD – Centralny Punkt Dystrybucyjny – najważniejszy element systemu okablowania strukturalnego; szafa 19”, w której zbiega się okablowanie pionowe i międzybudynkowe.</p> <p>BPD – Budynkowy Punkt Dystrybucyjny – spręga okablowanie z budynku do CPD</p> <p>KPD - Kondygnacyjny Punkt Dystrybucyjny – obejmuje piętra lub skrzydła budynku</p> <p>LPD – Lokalny Punkt Dystrybucyjny – przedłuża segment sieci</p>	<ul style="list-style-type: none"><li>• MDF - <i>Main Distribution Facility</i> – główny punkt dystrybucyjny, spełnia zadania PCS</li><li>• IDF – <i>Intermediate Distribution Facility</i> – pośredni punkt dystrybucyjny – stanowi odpowiednik BPD, KPD i LPD, w celu uporządkowania stosuje się kod cyfrowy</li><li>• POP – <i>Point Of Presence</i> – węzeł dostępu do internetu; fizyczne odwzorowanie miejsca w którym stoi urządzenie dostępowe (najczęściej w MDF)</li></ul>

# Punkt abonencki i oznaczenia

- **Punkt Abonencki (PA)** – ważny element SOS z punktu widzenia użytkownika sieci LAN: utożsamiany z fizycznym położeniem stanowiska pracy; (1PA na 10m<sup>2</sup>) i składa się z 2 gniazd RJ-45 i 3 gniazd elektrycznych do specjalnego przeznaczenia sieci elektrycznej, (ostatnio także 1 gniazdo światłowodowe)
  - **Sekwencja** określa porządek połączenia żył kabla do modularnych gniazd i wtyczek; w ramach SOS obowiązuje jeden rodzaj sekwencji !
  - **Polaryzacja** – definiuje fizyczny kształt oraz wymiary modularnych gniazd i wtyków, np. : WE8W (RJ-45), WE4W (RJ-11), WE6W (RJ-12)

Nr punktu dystrybucyjnego  
↓  
Nr kondygnacji → **01-105-44**  
↓  
Nr stelażu w szafie      Dwucyfrowy nr panelu  
↑  
Nr gniazda w panelu





## Podstawy Sieci Komputerowych

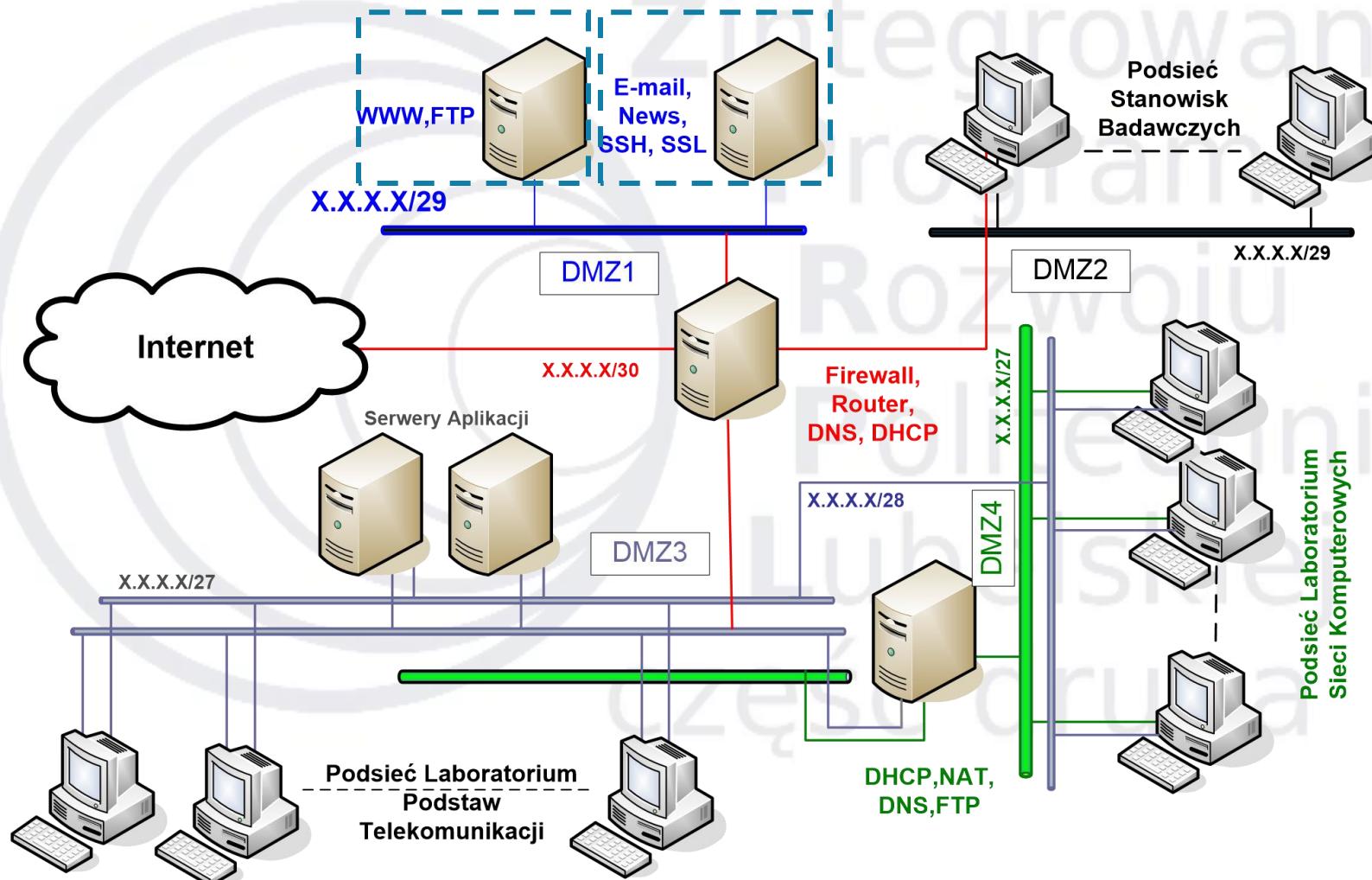
**Rodzina standardów IEEE 802.1 i IEEE 802.3**

**Typy i topologie sieci LAN. Sieci wirtualne VLAN**

**dr hab. inż. Konrad Gromaszek**



# Struktura małej sieci LAN



# Struktura sieci LAN

- Warunkiem wstępny podziału sieci lokalnej na warstwy jest poznanie jej atrybutów:
- **metodologii dostępu do zasobów LAN**, która opisuje sposób udostępniania zasobów przyłączanych do sieci; aspekt ten decyduje o jej typie:
  - **klient-serwer** (ang. *client-server*)
  - **równorzędny** (ang. *peer to peer*)
- **topologii sieci LAN**, która odnosi się do sposobu organizacji połączeń elementów składowych sieci i obejmuje dwa powiązane ze sobą terminy:
  - **topologia fizyczna** - zbiór zasad fizycznego łączenia poszczególnych urządzeń sieci ze sobą (układ przewodów, medium, połączenie hostów)
  - **topologia logiczna** - opisuje standardy z których powinna korzystać sieć podczas komunikacji. Topologie te definiuje najczęściej IEEE

# Topologia fizyczna

- Przykładowe topologie fizyczne:
  - **magistrali** (ang. *bus*) - wszystkie elementy sieci podłączone do jednej magistrali
  - **pierścienia** (ang. *ring*) - poszczególne elementy są połączone pomiędzy sobą odcinkami kabla tworząc zamknięty pierścień
  - **gwiazdy** (ang. *star*) - komputery są podłączone do jednego punktu centralnego, koncentratora (koncentrator tworzy fizyczną topologię gwiazdy, ale logiczną magistralę) lub przełącznika
  - **hierarchiczna** - zwana także topologią drzewa, jest kombinacją topologii gwiazdy i magistrali, budowa podobna do drzewa binarnego
  - **siatki** - oprócz koniecznych połączeń sieć zawiera połączenia nadmiarowe; rozwiązańe często stosowane w sieciach, w których jest wymagana wysoka bezawaryjność

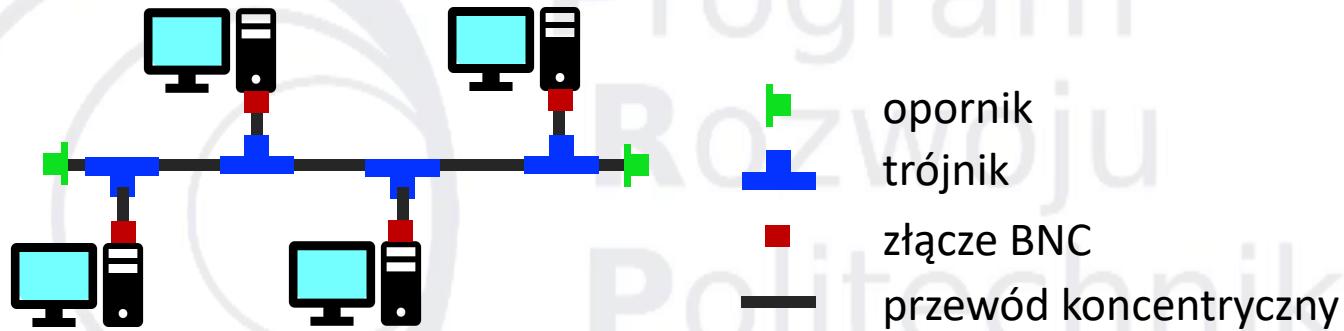
# Topologia logiczna

- **Topologia logiczna**
  - opisuje reguły komunikacji, z których powinna korzystać każda stacja robocza przy komunikowaniu się w sieci
  - poza połączeniem fizycznym hostów i ustaleniem standardu komunikacji, zapewnia bezbłędną transmisję danych.
  - topologia fizyczna jest ścisłe powiązana z topologią logiczną
- Niektóre topologie fizyczne wraz z wybranymi topologiami logicznymi:

Topologie fizyczne	Topologie logiczne
gwiazdy i magistrali	IEEE 802.3 - 10 Mb Ethernet
	IEEE 802.3u - 100 Mb Ethernet
	IEEE 802.3z - 1 Gb Ethernet
pierścienia	IEEE 802.5 - Token ring
	FDDI

# Topologie proste (1/3)

- **Topologia magistrali**



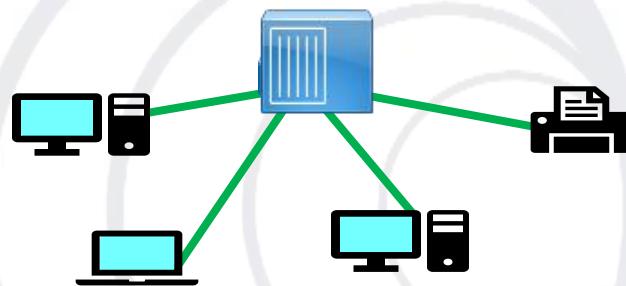
- **Topologia pierścienia**

Poważną wadą jest  
zaprzestanie pracy **całego**  
pierścienia w przypadku awarii  
**jednej** stacji roboczej



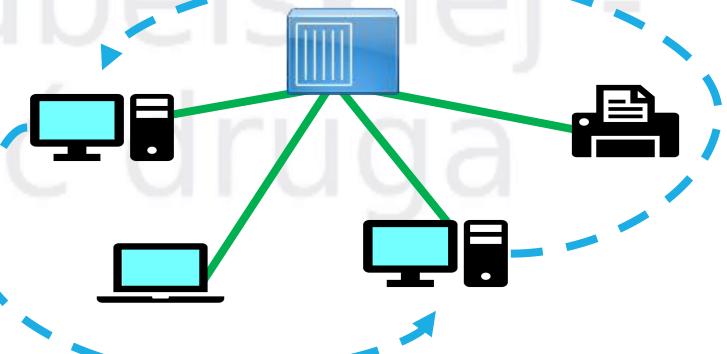
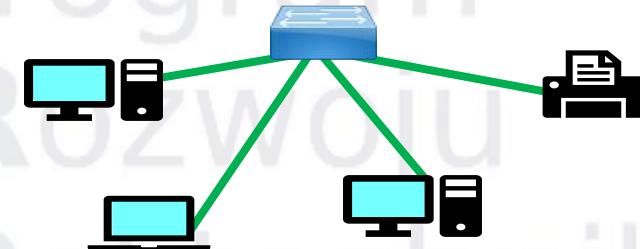
# Topologie proste (2/3)

- **Topologia gwiazdy**



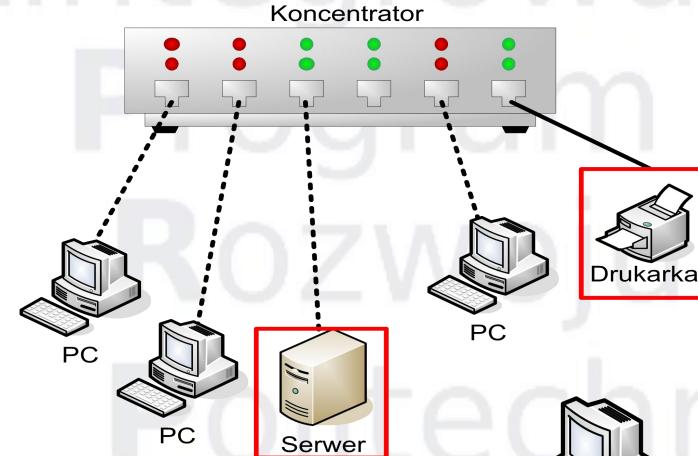
- **Topologia pierścienia *Token Ring*-(gwiazda z dostępem cyklicznym)**

linie przerywane reprezentują logiczny przebieg dostępu do nośnika



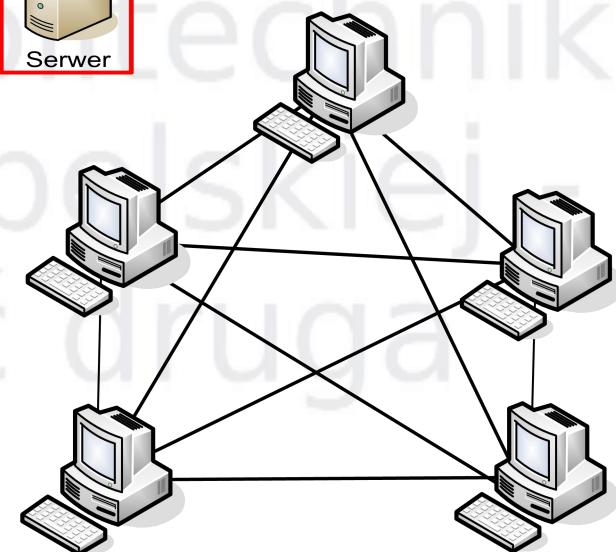
# Topologie proste (2/3)

- **Topologia przełączana**

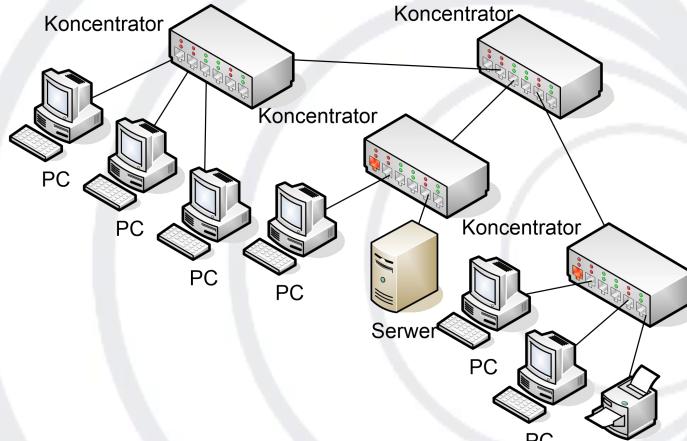


- **Topologia siatki (oczkowa)**

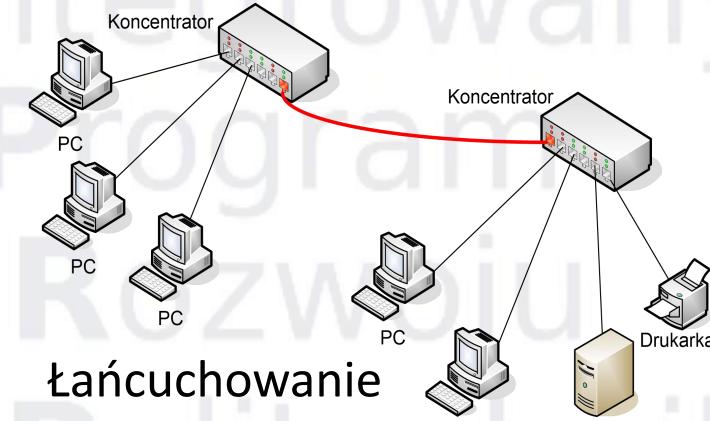
Siatka częściowa jest zastosowana w schemacie Internetu, gdzie istnieje wiele ścieżek do dowolnego miejsca, chociaż nie ma tu połączeń między wszystkimi hostami



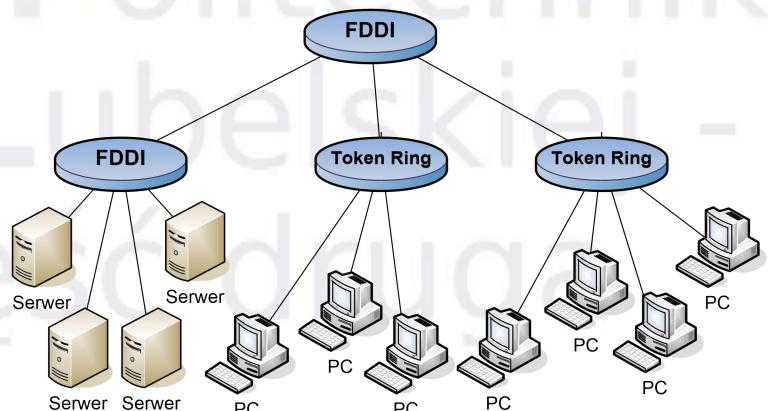
# Topologie złożone



Hierarchiczne gwiazdy

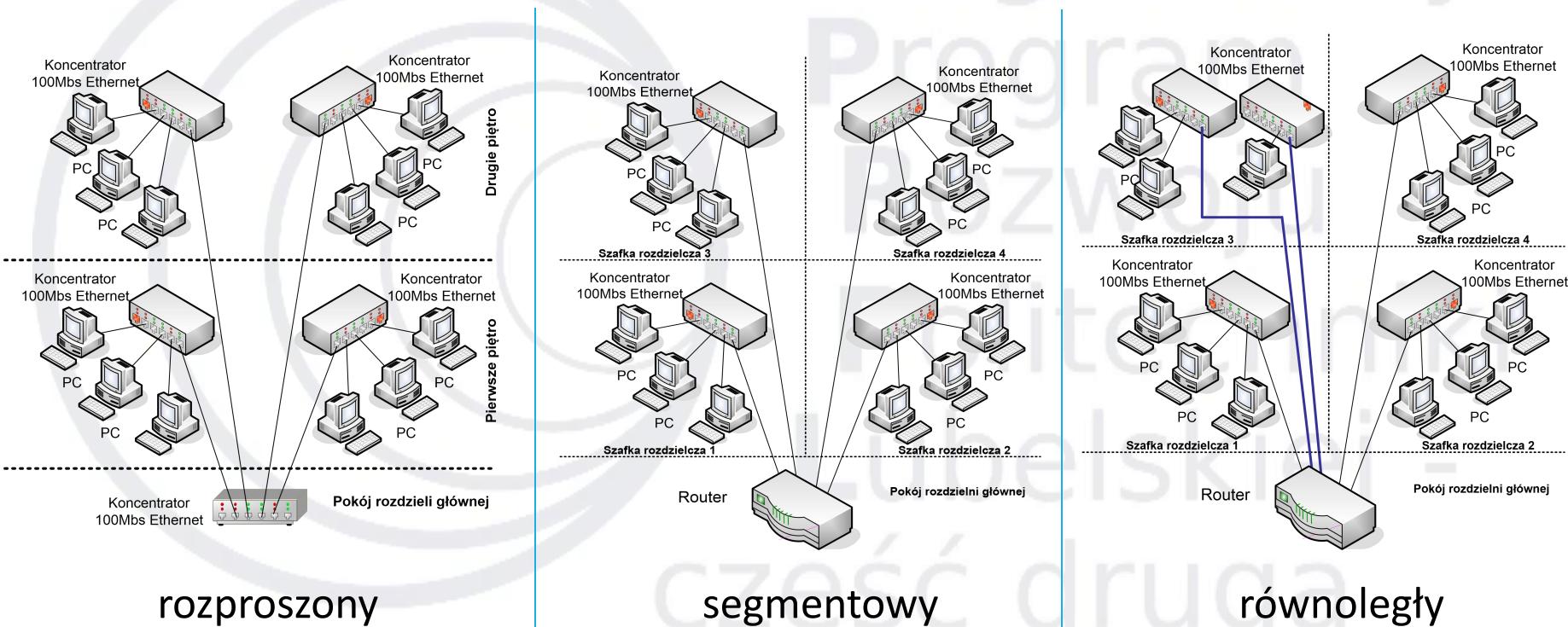


Łańcuchowanie



Hierarchiczne pierścienie

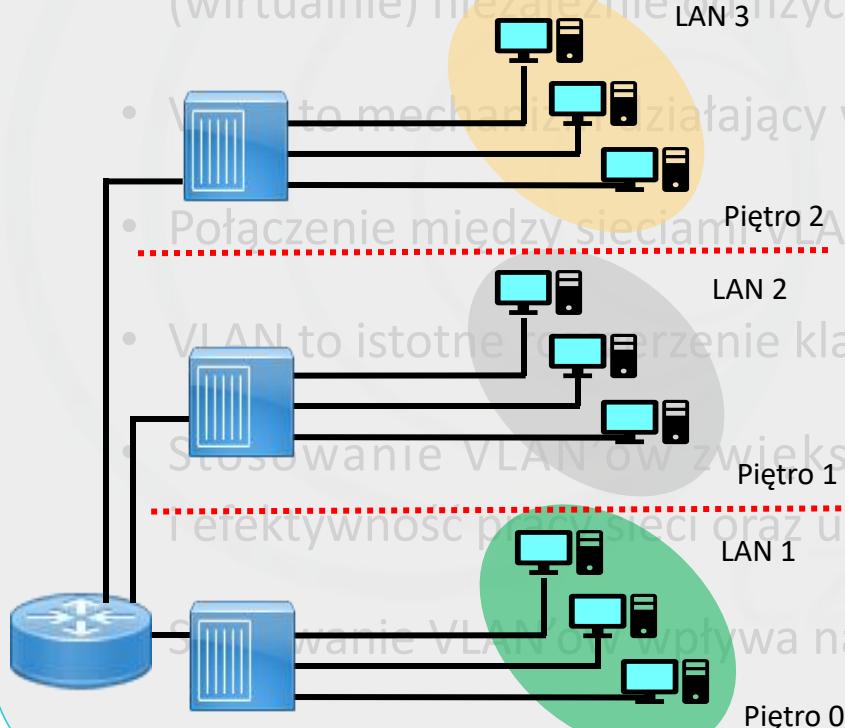
# Od szkieletu do VLAN



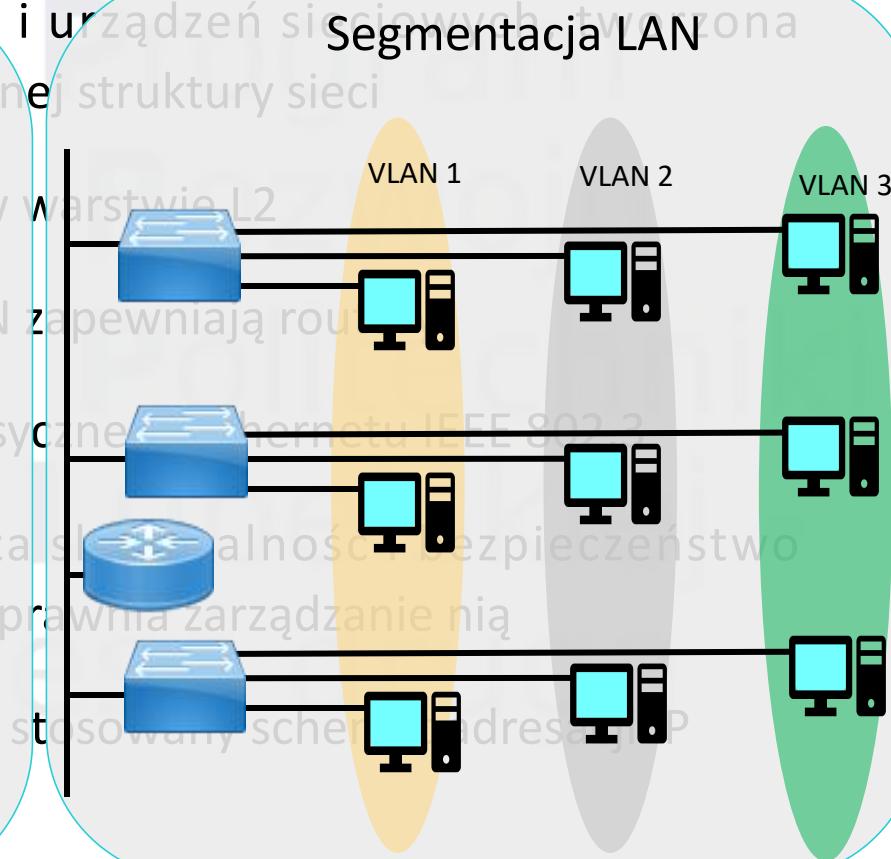
# Wirtualne LAN

## Tradycyjna segmentacja LAN

(wirtualnie) niezależnie od fizycznej struktury sieci



## Segmentacja LAN

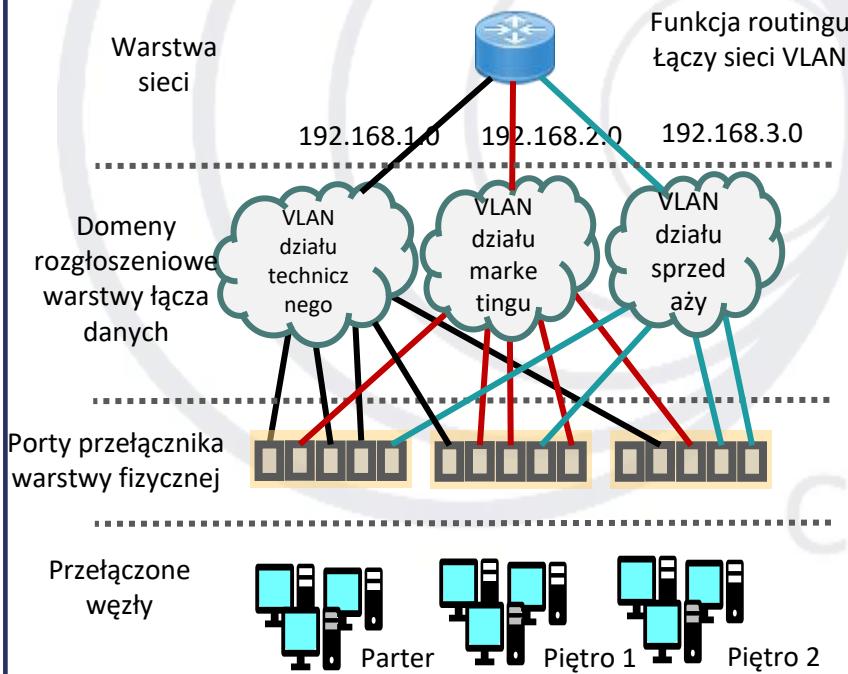


# Rodzaje sieci VLAN

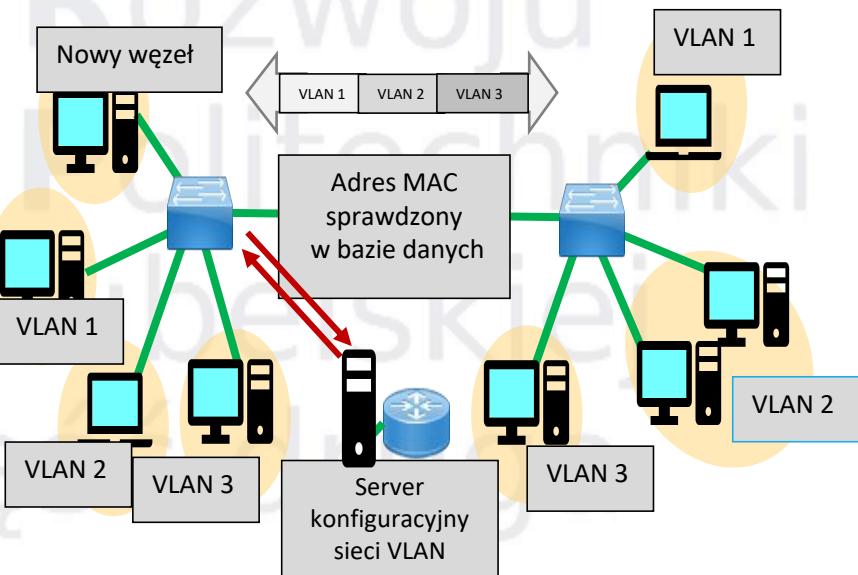
- Można wyróżnić dwa rodzaje sieci VLAN:
  - Statyczne – administrator konfiguruje je dla każdego portu; każdy port jest przypisywany do konkretnej sieci VLAN
  - Dynamiczne – porty mogą dynamicznie określić konfigurację swoich VLAN; korzystają w tym celu z przygotowanej bazy odwzorowań adresów MAC na sieci VLAN, którą wcześniej przygotowuje administrator

# Rodzaje sieci VLAN

## Statyczne



## Dynamiczne

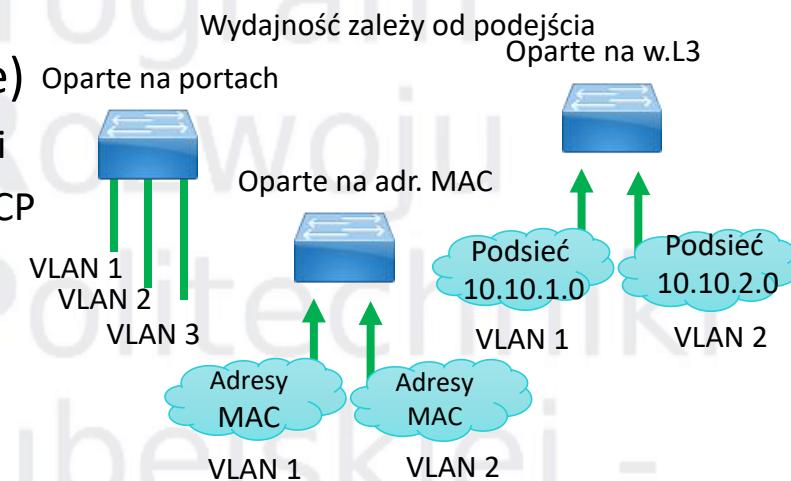


# Przynależność do VLAN

- Ze względu na określenie przynależności wyróżnia się VLAN:

- VLAN oparte na portach (statyczne)**

- Najpopularniejsza metoda konfiguracji
- Stosowana w sieciach protokołem DHCP
- Łatwe w użyciu



- VLAN oparte na adresach MAC**

- Rzadziej stosowane
- Wymaga ręcznej konfiguracji każdego adresu na przełączniku
- Trudne w administrowaniu i zarządzaniu

- VLAN oparte na protokołach**

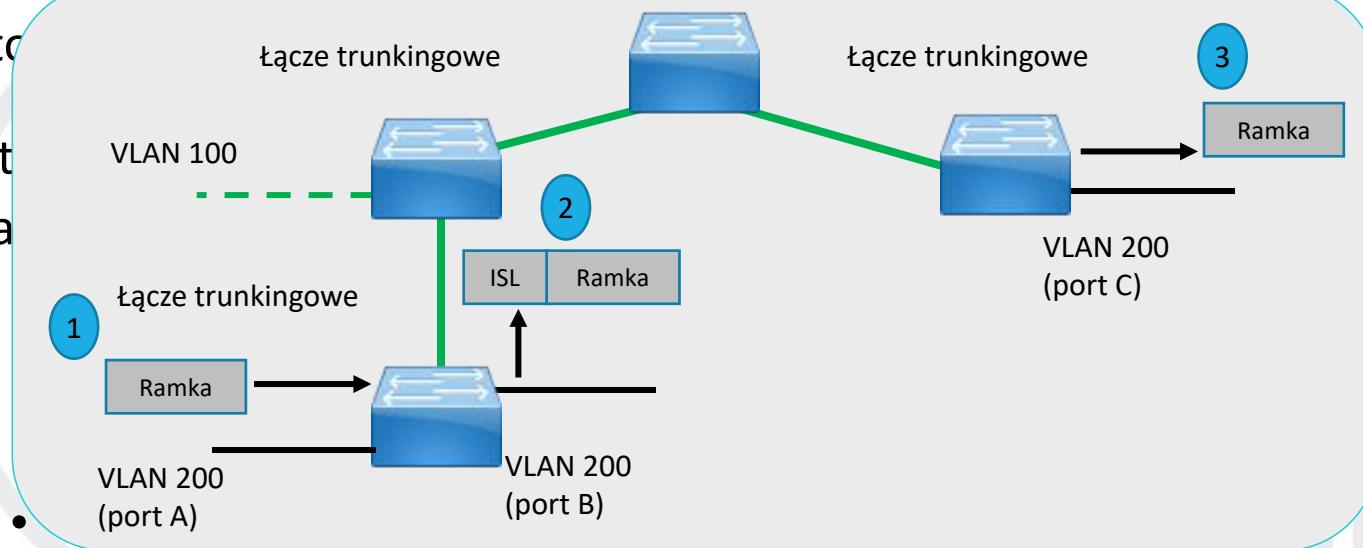
- Konfiguracja jak dla adresów MAC, ale używany jest adres logiczny
- Rzadziej stosowane ze względu na DHCP

# Łącza trunk

- **Łącza trunkingowe** to fizyczne i logiczne połączenie między przełącznikami, po którym odbywa się ruch w sieci
- Rozróżnienie przynależności ramek do poszczególnych VLANów realizuje się przez **znakowanie ramek** lub **filtrowanie ramek**
  - **Filtrowanie ramek** – przełączniki wymieniają się zawartością tablic adresów (podobny schemat jak ten wykorzystywany przez routery)
  - **Znakowanie ramek** – każda ramka wysyłana za pośrednictwem łącza jest znakowana informacjami od sieci VLAN, do której należy

# Znakowanie ramek (tagowanie)

- Stopnie znakowania ramek
- Istotne dla VLAN
- Współczesne technologie LAN

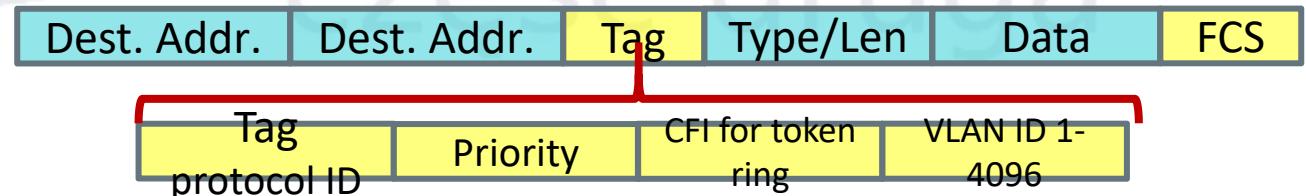


dwa  
to:  
mkę

Zwykła ramka



Ramka z 4B  
znacznikiem,  
przeliczone FCS



# Protokół VTP

- **VTP (*VLAN Trunking Protocol*)** – protokół Cisco, który zapewnia obsługę dynamicznego informowania o dodaniu, usunięciu i zmianie nazwy sieci VLAN w całej strukturze przełącznika, używając ramek łączy trunkingowych
- Zalety:
  - Spójność konfiguracji sieci VLAN w całej sieci
  - Tworzenie łączy trunk w środowiskach o mieszanych nośnikach
  - Dokładne śledzenie i monitorowania sieci VLAN
  - Dynamiczne informowanie o nowych VLANach w sieci
  - Możliwość dodawania nowych VLAN w trybie plug-and-play
- Wykorzystuje domenę VTP, która składa się z 1 lub więcej urządzeń, posiadających wspólną domenę VTP



## Podstawy Sieci Komputerowych

### Rodzina standardów IEEE 802.1 i IEEE 802.3

Mechanizmy dostępu do medium. Standard IEEE802.

Technologia Ethernet i inne standardy.

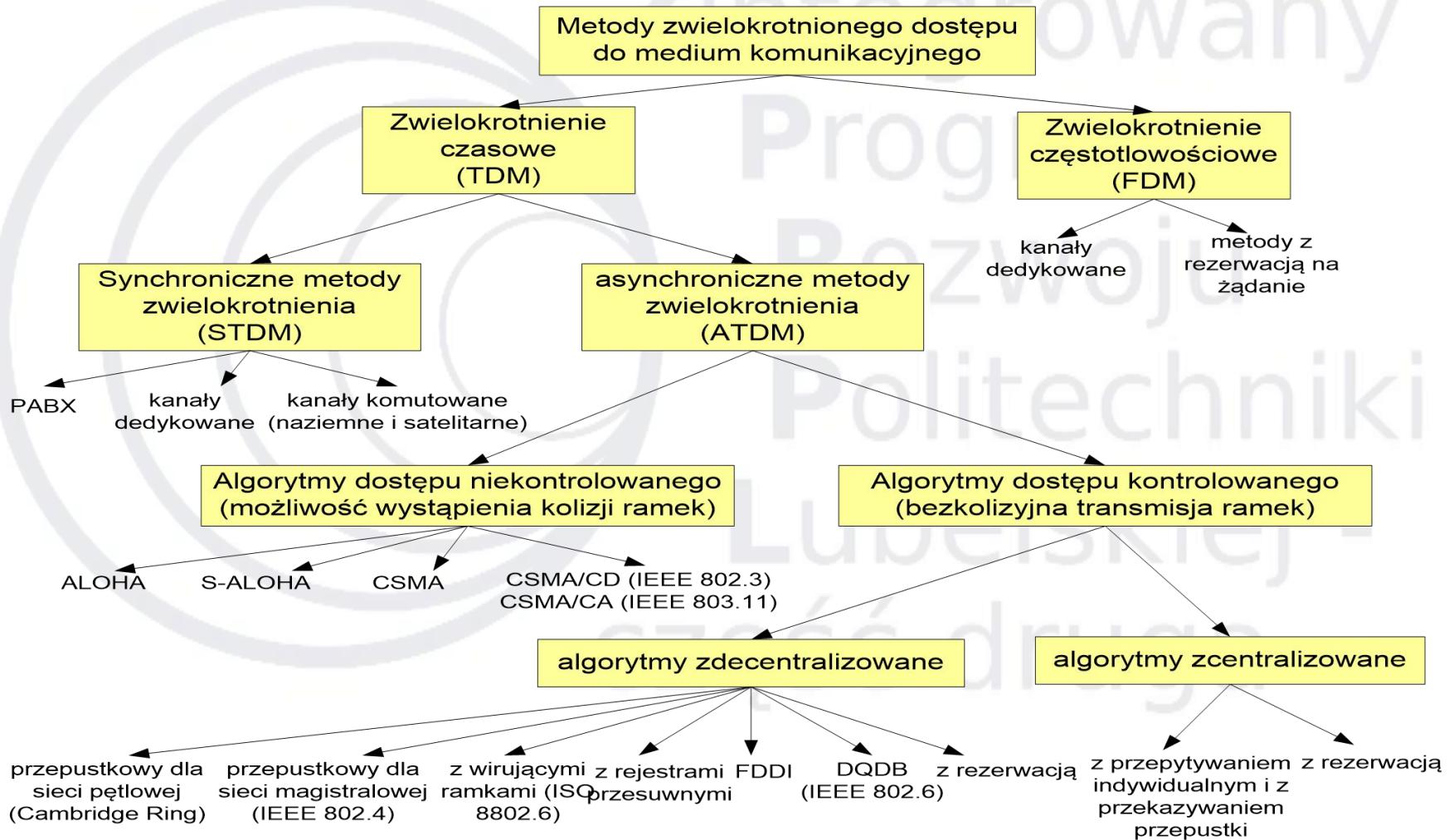
dr hab. inż. Konrad Gromaszek



# Dostęp do medium komunikacyjnego

- Każda sieć musi w jakiś sposób regulować dostęp do medium komunikacyjnego
- Mechanizm taki realizowany jest przez warstwę łącza danych
- Potrzeba sterowania dostępem do medium może być realizowana w różny sposób :
  - na zasadzie **rywalizacji**
  - w formie **przesyłania tokenu**
  - w formie **Priorytetu żądań**
  - Na zasadzie **przełączania**

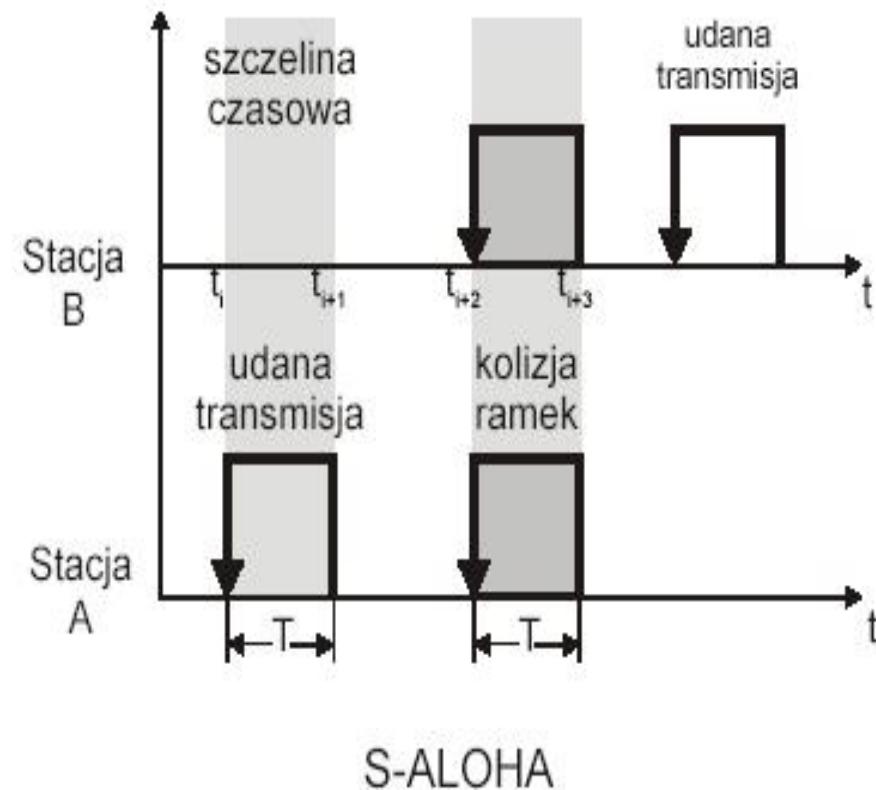
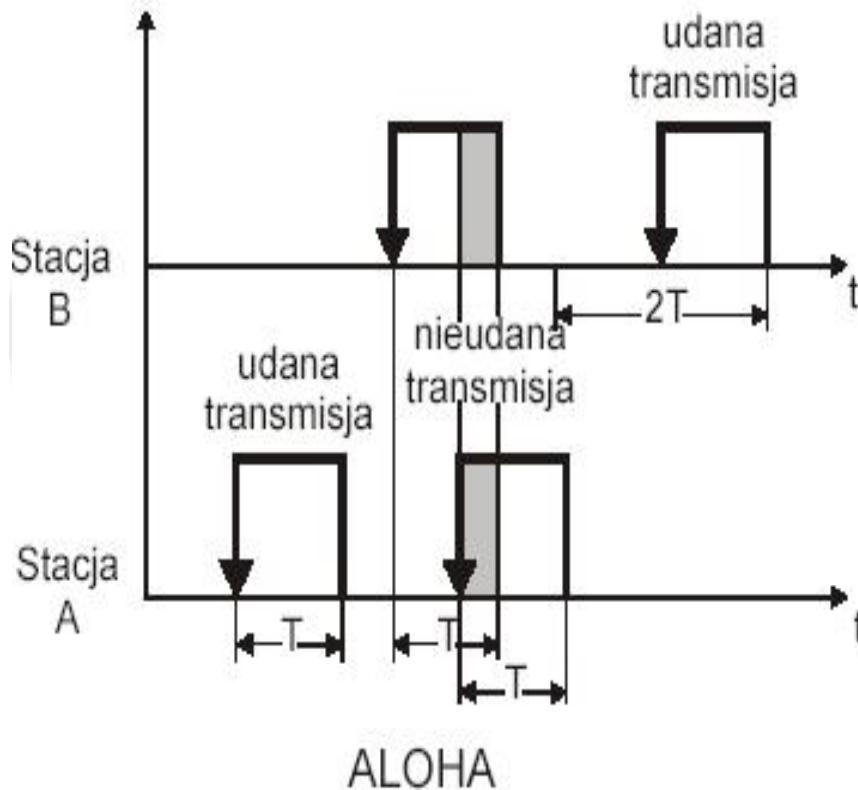
# Metody dostępu do medium



# Dostęp w oparciu o rywalizację

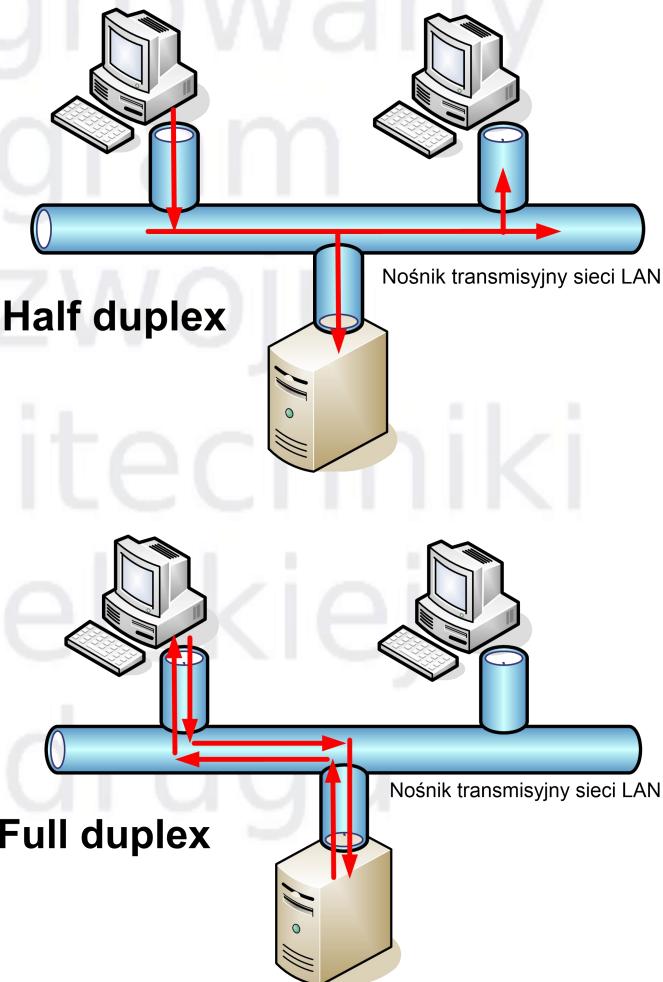
- Dostęp do medium na zasadzie rywalizacji:
  - Wszystkie urządzenia konkurujące ze sobą o dostępne pasmo tworzą **domenę kolizji**
  - Każde urządzenie dołączone do sieci przyjmuje na siebie ciężar **samodzielnego przeprowadzenia transmisi**
  - Prosty sposób regulowania dostępu, bo nie posiada on **żadnych scentralizowanych mechanizmów** regulacyjnych
- Za każdym razem, kiedy urządzenie chce przesyłać dane, musi sprawdzić, czy kanał transmisyjny jest wolny. W przeciwnym razie, urządzenie, które potrzebuje wysłać dane, musi swój zamiar porzucić i odczekać określony przedział czasu przed podjęciem ponownej próby wysłania

# Protokół ALOHA i S-ALOHA

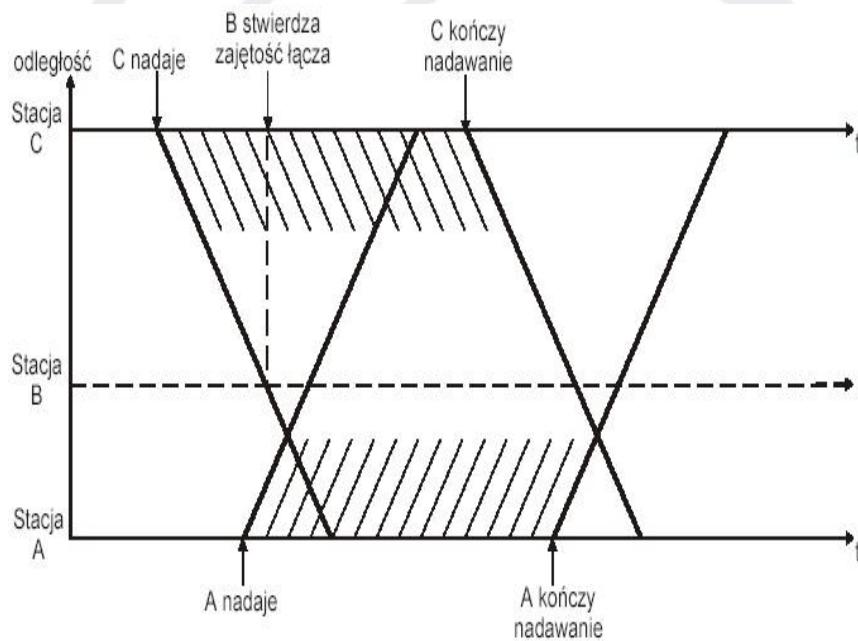


# Tryby pracy łącza LAN

- Łącza LAN mogą pracować w następujących trybach:
  - Simplex** - tylko jedno urządzenie może przesyłać dane w danej chwili
  - Half-duplex** (półduplex) - urządzenie może odbierać, albo wysyłać dane, ale nigdy obie te *czynności nie występują jednocześnie*
  - Full duplex** – w trybie tym dostępna szerokość pasma jest podzielona na odrębne kanały, umożliwiając „jednoczesną” dwukierunową transmisję

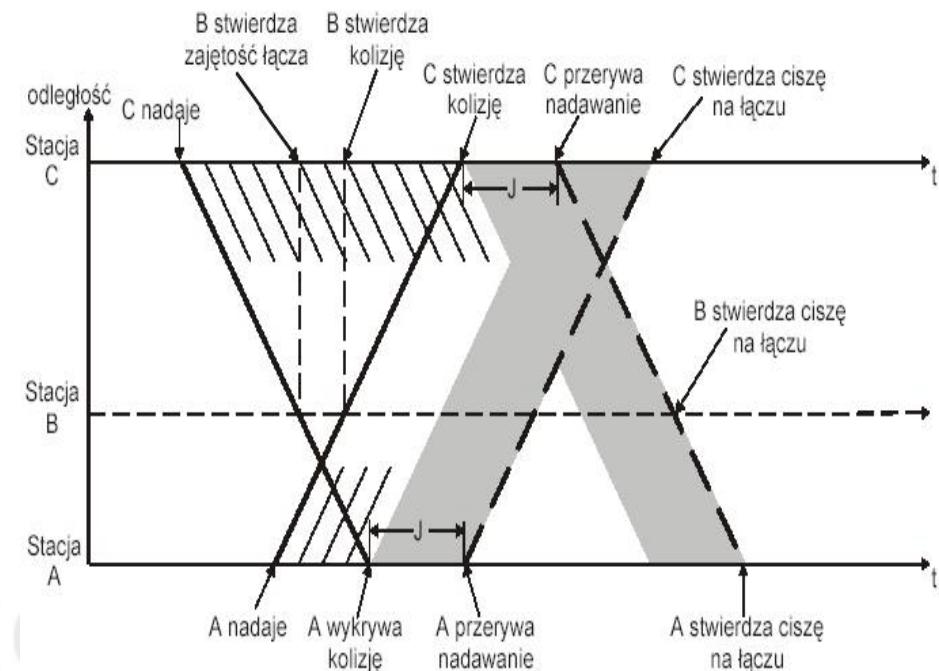


# Dostęp rywalizacyjny CSMA/CD



**CSMA**

Źródło rys.: Tanenbaum A. S., Wetherall D. J., Sieci komputerowe, wyd. 5, Helion, Gliwice, 2012



**CSMA/CD**

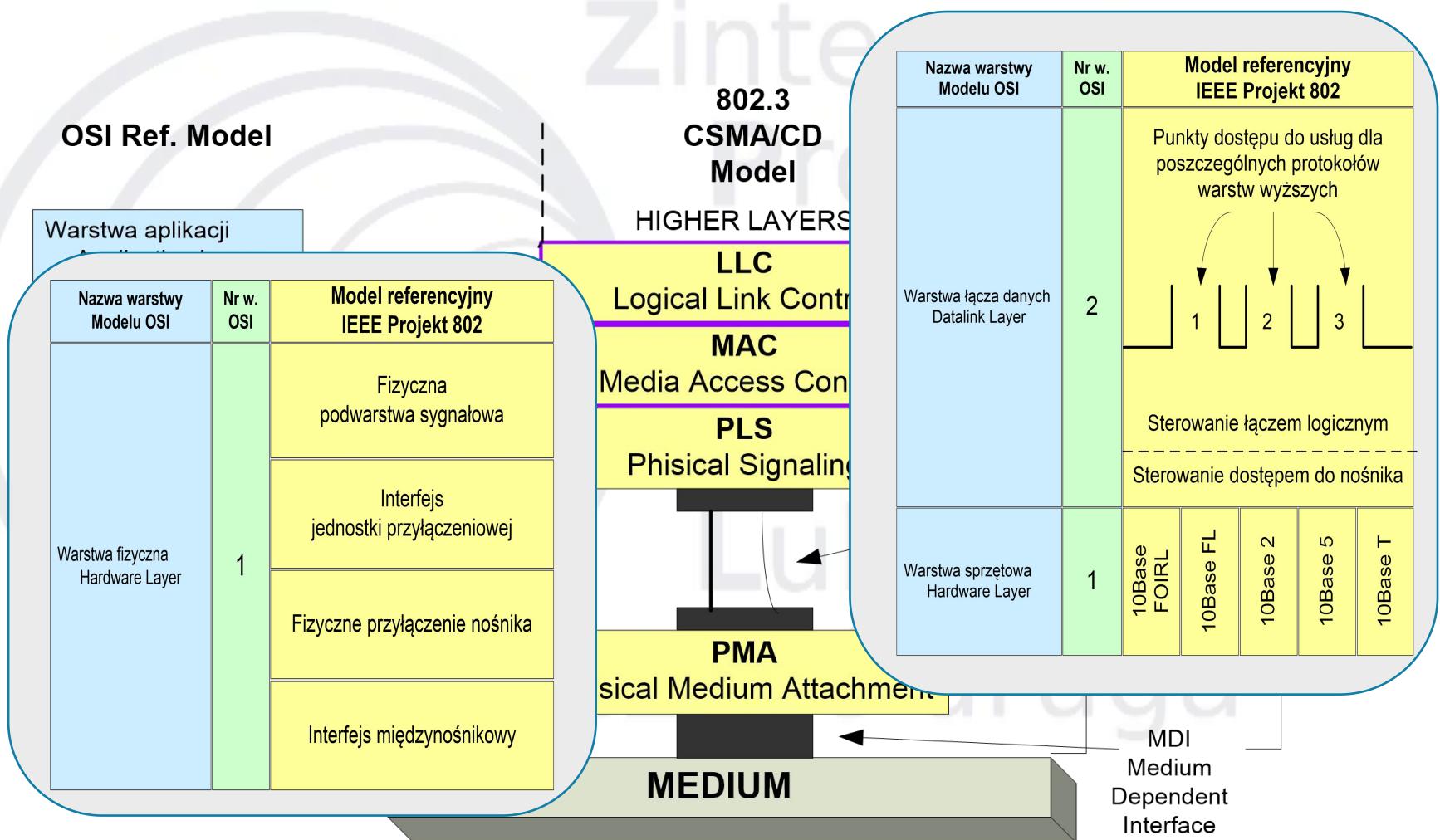
# Dostęp w oparciu o token

- Alternatywny sposób dostępu do medium, charakterystyczny dla sieci LAN opartych na topologii pierścienia: Token Ring i FDDI
- Token (żeton) to specjalna ramka, która jest przesyłana w jednym kierunku do kolejnych urządzeń wchodzących w skład pierścienia
- Token uznawany jest przez wszystkie urządzenia za element decydujący o dostępie do medium komunikacyjnego
- urządzenie musi posiadać token aby umieścić jakiekolwiek dane w sieci
- Token może być przesyłany tylko wtedy, gdy sieć jest wolna
- Sieci oparte na przesyłaniu tokenu nadają się do zastosowań wymagających przewidywalnej wartości opóźnień

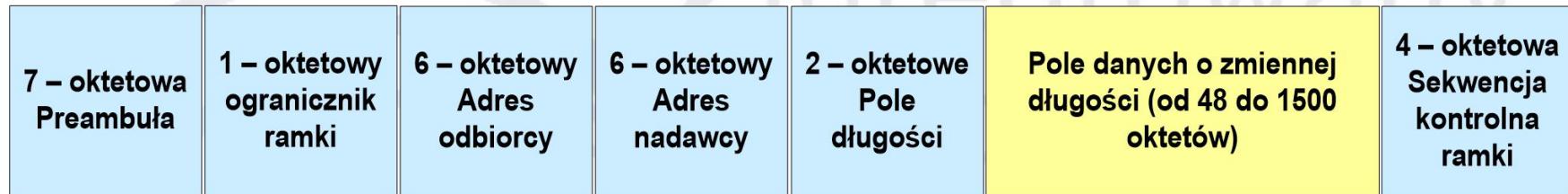
# Dostęp w formie priorytetu żądań

- Metoda dostępu **na zasadzie priorytetu żądań** była wykorzystywana w sieciach odpowiadających specyfikacji IEEE 802.12 100 Mbps o ramkach formatu Token Ring lub Ethernet oraz topologii gwiazdy
- Jest to metoda **cyklicznego przyznawania prawa dostępu**, w której **centralny wzmacniak** (koncentrator) regularnie sprawdza stan **przyłączonych do niego portów**
- Sprawdzanie to wykonywane jest w kolejności portów i ma na celu określenie, które z nich zgłaszą żądania transmisji
- Po rozpoznaniu zgłoszenia koncentrator określa jego priorytet, który może być normalny lub wysoki wynikający z potrzeby uprzywilejowanego dostępu do medium procesom, które obsłużone muszą być w określonym czasie
- Stosowana w VG-AnyLAN (*voice grade wiring, any LAN architecture*), nie dotrzymała kroku prostrzym CSMA/CD w Fast Ethernet

# IEEE 802.3 a model OSI



# Ramki Ethernet



IEEE 802.3 z podramką LLC



IEEE 802.3 z podramką SNAP



# Standard Fast Ethernet

- W początku lat 90. wprowadzono pewne modyfikacje do tradycyjnych rozwiązań sieci Ethernet wynikające głównie z pojawienia się technologii ATM => Fast Ethernet i VG-AnyLAN
- W praktyce szerokie zastosowanie znalazła technologia Fast Ethernet, posługująca się CSMA/CD w dostępie do medium
- Fast Ethernet został znormalizowany jako rozszerzenie istniejącego standardu 802.3: zachowano w nim protokoły warstwy łączą danych przy zwiększonej dziesięciokrotnie prędkości przesyłania sygnału
- W celu sprostania wymaganiom standardu należało zmodyfikować warstwę fizyczną poprzez dodanie nowych specyfikacji interfejsów:
  - 100BaseTX
  - 100BaseFX
  - 100BaseT4

# Standard Gigabit Ethernet

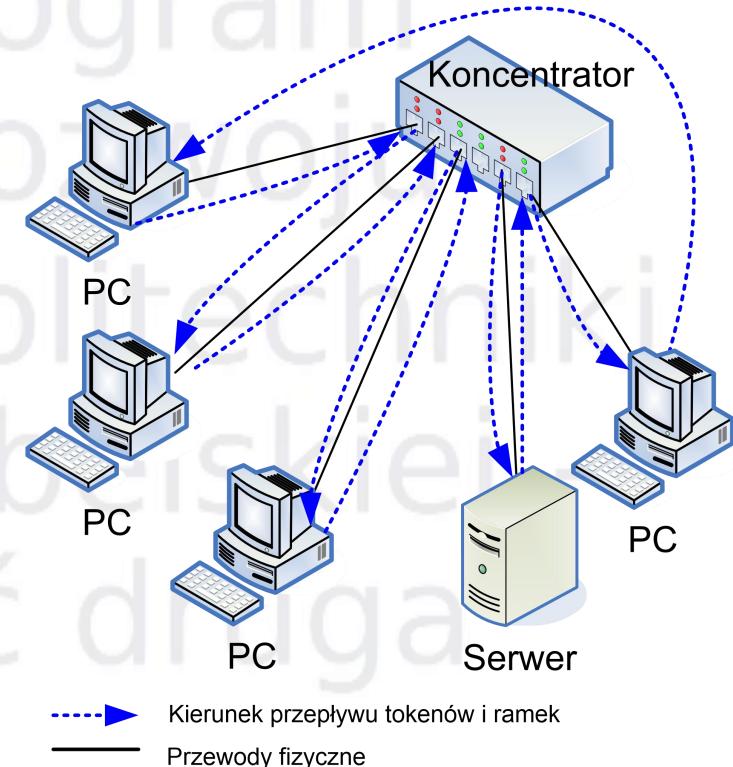
- Gigabit Ethernet **IEEE 802.3z** miał początkowo służyć jako szkielet łączący ze sobą przełączniki 10/100BaseT oraz do łączenia wysokowydajnych serwerów z siecią LAN
- Jako ratyfikowany standard **IEEE 802.3ab**, stosunkowo szybko zaczął służyć do łączenia stacji roboczych za pomocą kabli UTP Kategorii 5, lub 6 w segmentach do 100 m
- Gigabit Ethernet pozwala na wybór pomiędzy czterema nośnikami, z których każdy ma własną specyfikację interfejsu fizycznego:
  - miedziany kabel koncentryczny
  - wielofunkcyjny kabel światłowodowy
  - jednomodowy kabel światłowodowy 9/125 µm
  - skrętka dwużylowa (UTP) Kategorii >5

# Standard 10Gigabit Ethernet

- **10 Gigabit Ethernet** (10GE, 10GbE lub 10 GigE) jest technologią wykorzystywaną w sieciach komputerowych, określającą standardy transmisji ramek Ethernetowych z prędkością 10 Gb/s.
- Zdefiniowany w **IEEE 802.3ae** w 2002 i obsługuje połączenia wyłącznie w trybie pełnego dupleksu (w przeciwieństwie do poprzednich standardów Ethernet), czego następstwem jest brak wsparcia CSMA/CD (brak możliwości stosowania koncentratorów)

# Standard IEEE 802.5 - TokenRing

- Dostęp do medium jest przyznawany poprzez przekazywanie **tokenu w ustalony sposób**
  - Token może być tylko **jeden** i jest on modyfikowany przez urządzenie transmitujące w celu utworzenia nagłówka ramki danych
  - Urządzenie odbierające **kopiuje** dane przesyłane w ramce, **zmieniając** przy tym (negując) niektóre **bity nagłówka ramki** i w ten sposób potwierdzając odbiór
  - Urządzenie, które wysłało ramkę, **pobiera** ją teraz z sieci i **usuwa** z niej dane oraz adresy.
  - Jeśli urządzenie chce przesłać więcej danych, może to zrobić
  - Jeśli nie, nagłówek ramki jest **przekształcany** z powrotem w token i **umieszczany w medium transmisyjnym**, przez które przesyłana jest do następnego urządzenia



# Ramka IEEE 802.5 - TokenRing

- Struktura ramki 802.5 Token Ring składa się z dwóch części: tokenu i ramki danych



- Ramki tokenów i ramki danych mają trzy takie same 1-oktetowe pola:
  - ogranicznika początku
  - sterowania dostępem
  - ogranicznika końca
- Pole **Sterowania dostępem** jest kluczowe dla działania Token Ring
- Zawiera ono osiem bitów, z których jeden musi zostać odwrócony w celu dezaktywacji tokenu i zamiany go na sekwencję początku ramki

# Ramka FDDI

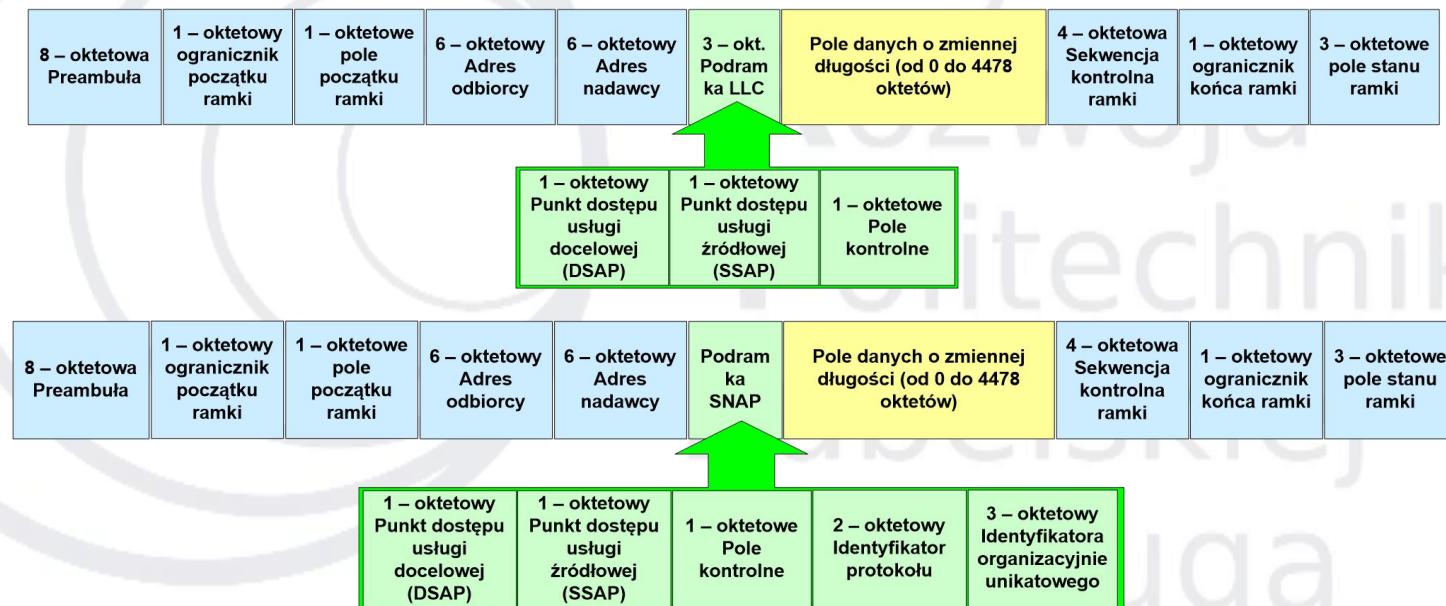
- Oficjalna nazwa tej standardowej architektury sieci LAN opracowanej przez amerykański instytut ANSI brzmi „*Fiber Distributed Data Interface*” (Złącze Danych Przenoszonych Światłowodem).

8 – oktetowa Preambuła	1 – oktetowy ogranicznik początku ramki	1 – oktetowe pole początku ramki	6 – oktetowy Adres odbiorcy	6 – oktetowy Adres nadawcy	Pole danych o zmiennej długości (od 0 do 4478 oktetów)	4 – oktetowa Sekwencja kontrolna ramki	1 – oktetowy ogranicznik konca ramki	3 – oktetowe pole stanu ramki
---------------------------	--	---	-----------------------------------	----------------------------------	--	---	--	-------------------------------------

- Zwykle z ramki FDDI korzysta się w połączeniu z jednym z dwóch podformatów: LLC lub SNAP
- Ramka o tak utworzonym formacie również nie może mieć więcej niż 4500 oktetów (nie licząc Preambuły)

# Podramki FDDI LLC i SNAP

- Ramka FDDI może zawierać struktury podramki 802.2 LLC, na które składają się pola DSAP, SSAP oraz Pole kontroli



- Ramka SNAP dodaje do struktur podramki 3-oktetowe pole Identyfikacji protokołu oraz 2-oktetowe pole Typu.

**POLITECHNIKA LUBELSKA**

**WYDZIAŁ ELEKTROTECHNIKI I INFORMATYKI**

**INFORMATYKA**



Zintegrowany  
Program  
Rozwoju  
Politechniki  
Lubelskiej -  
część druga

## Podstawy Sieci Komputerowych

**Rodzina standardów IEEE 802.1 i IEEE 802.3**  
**Protokół STP i RSTP**

dr hab. inż. Konrad Gromaszek



**Fundusze  
Europejskie**  
Wiedza Edukacja Rozwój



**Rzeczpospolita  
Polska**

**Unia Europejska**  
Europejski Fundusz Społeczny

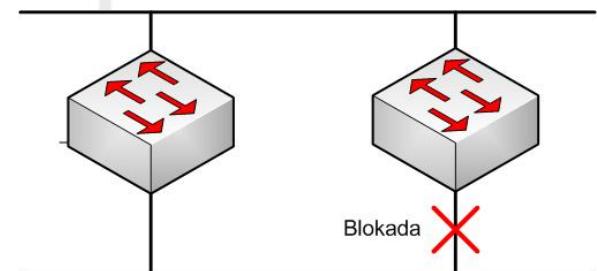


# Konsekwencje nadmiarowości w sieciach LAN

- Ma w sieci krytyczne znaczenie pod względem niezawodności
- Gwarantuje odporność sieci na błędy
- Chroni przed przestojami w pracy sieci lub niedostępnością (administracyjna kwestia kompromisu pomiędzy kosztem nadmiarowości a zapotrzebowaniem dostępności sieci)
- Musi być ostrożnie planowana i monitorowana ze względu na podatność na:
  - burze rozgłoszeniowe,
  - transmisje wielu kopii tych samych ramek,
  - niestabilność bazy danych adresów MAC
- Wymagana do ochrony przed utratą łączności z powodu awarii pojedynczego elementu

# Spanning Tree Protocol

- **Zbieżność** w STP – stan, w którym wszystkie porty przełączników i mostów weszły w stan przekazywania lub blokowania. Jest ona konieczna do normalnej pracy sieci
- Czas potrzebny na realizację zbieżności – kluczowa kwestia po wystąpieniu zmian w topologii sieci
- Normalny czas zbieżności dla STP IEEE802,1d = 30-50 sek.
- Przechodząc do logicznej topologii bez pętli STP wykorzystuje dwa kluczowe mechanizmy:
  - **Identyfikator mostu** (ang. *Bridge ID, BID*)
  - **Koszt ścieżki** (ang. *path cost*)



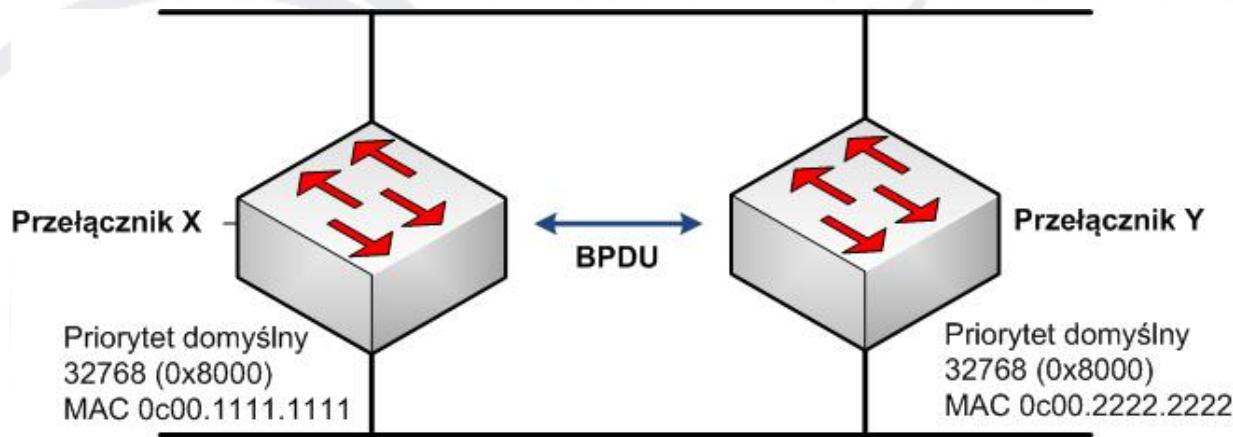
# Spanning Tree Protocol - BID

- **Identyfikator mostu** (ang. *Bridge ID, BID*) – składa się z priorytetu i adresu MAC mostu



- Przełączniki i mosty wykonujące algorytm drzewa rozpinającego regularnie wymieniają z innymi przełącznikami i mostami komunikaty zawierające konfigurację (co 2 sek.) pomocą grupowej ramki **BPDU** (ang. *bridge protocol data unit*), z których jedna z informacji to **BID**
- STP wymaga przypisania niepowtarzalnego BID każdemu przełącznikowi i mostowi
- Domyślny priorytet wg. IEEE 802.1d ma wartość ze środka zakresu 32768 (0x8000hex)
- Główny most ma najniższy identyfikator BID

# Spanning Tree Protocol - BID



- STP wymaga przypisania niepowtarzalnego BID każdemu przełącznikowi i mostowi
- Domyślny priorytet wg. IEEE 802.1d ma wartość ze środka zakresu 32768 (0x8000hex)
- Główny most ma najniższy identyfikator BID

# STP – koszt ścieżki

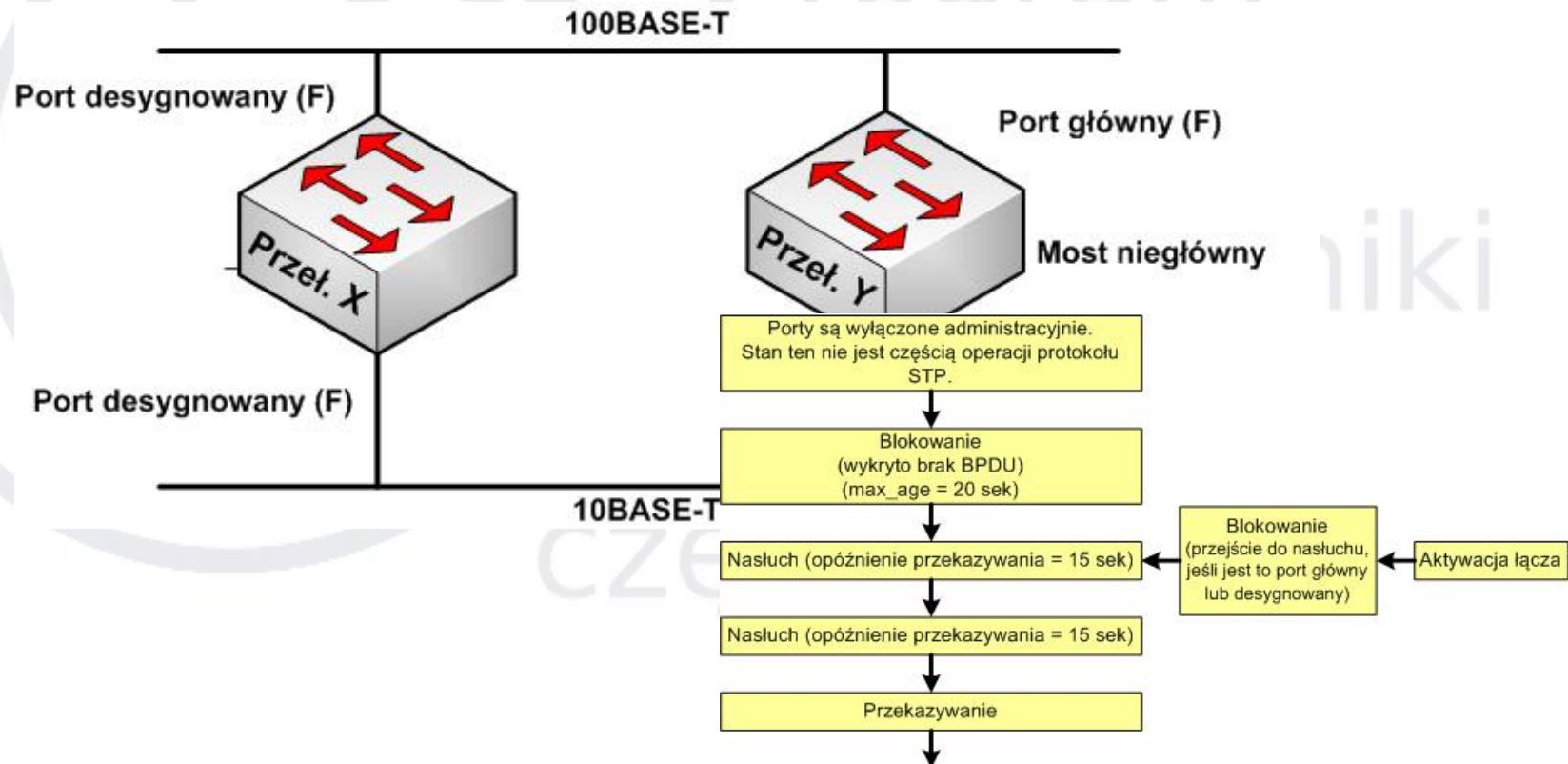
- Najkrótsza ścieżka jest wybierana na podstawie łącznych kosztów łącza, które z kolei są oparte na jego szybkości
- Koszt ścieżki drzewa rozpinającego, to koszt całkowity, bazujący na szerokości pasma wszystkich łącz w ścieżce

Łącze	Koszt STP IEEE802.1d	Koszt STP
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

- W specyfikacji IEEE802.1d stosowana jest skala nieliniowa, uwzględniając szybsze interfejsy
- Im niższy koszt wyznaczony w STP, tym lepsza ścieżka

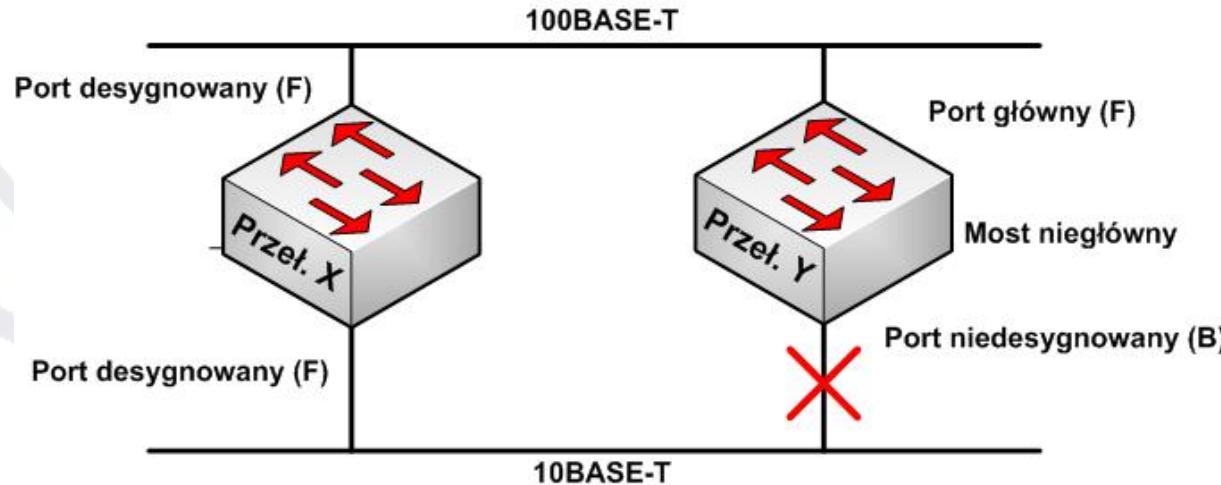
# Realizacja zbieżności w logicznej topologii bez pętli

- Procedura

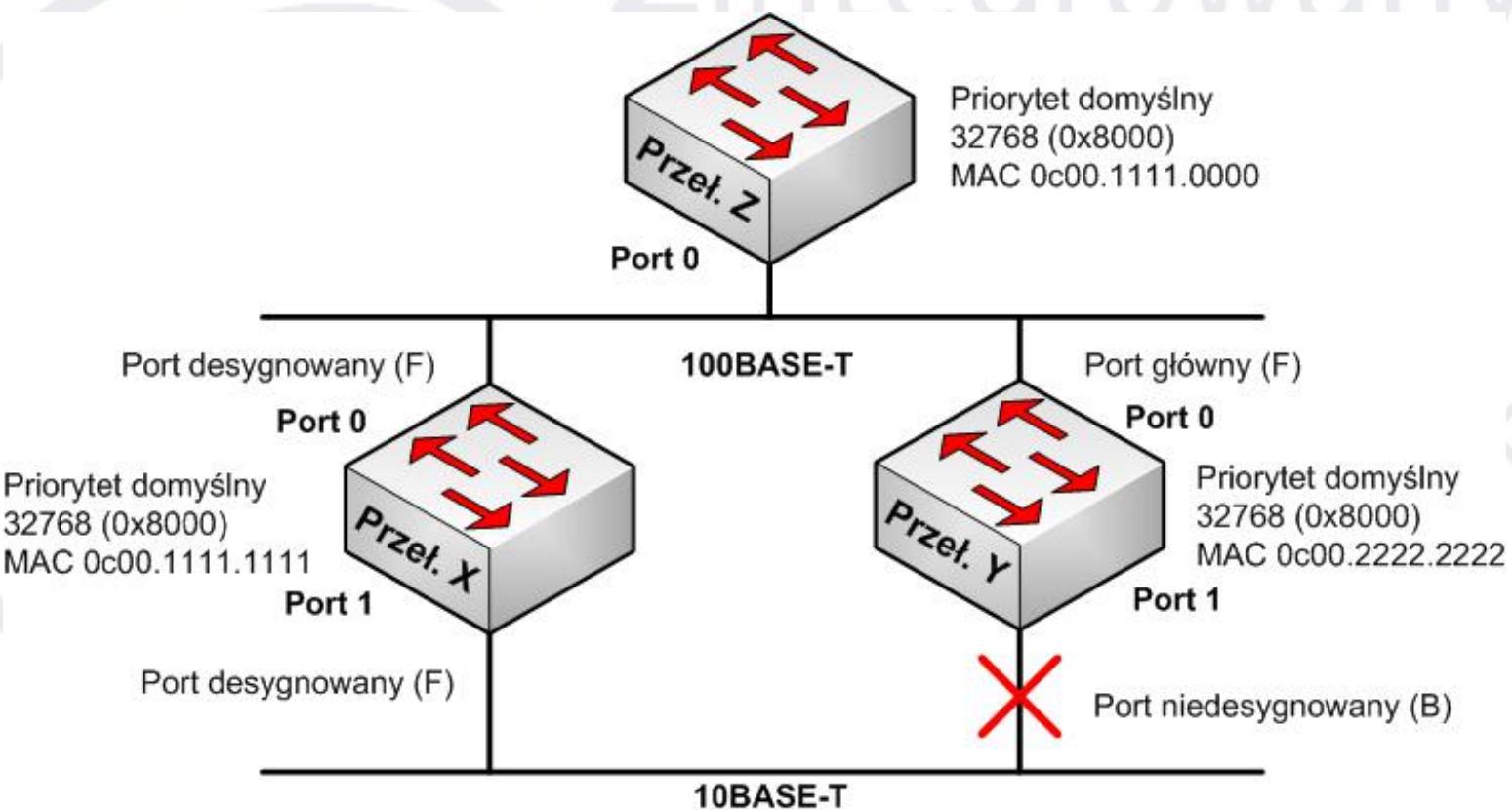


# Funkcja PortFast

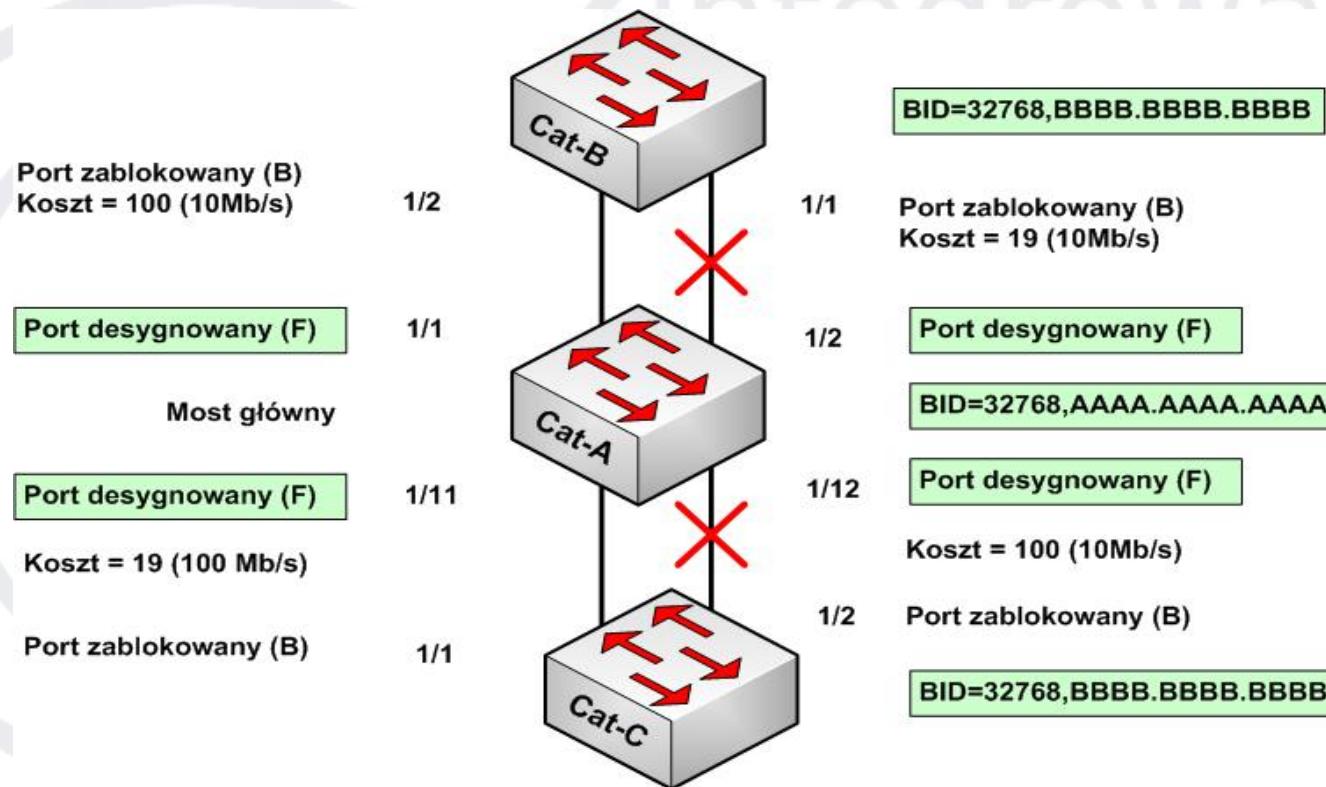
- Funkcja **PortFast** – pozwala przy pierwszym uruchomieniu na automatyczne przejście do ze stanu blokowania do stanu przekazywania; dopuszczalne ze względu na fakt, że port nie może brać udziału w tworzeniu pętli, ponieważ nie jest połączony z żadnym przełącznikiem ani mostem



# Przykład STP



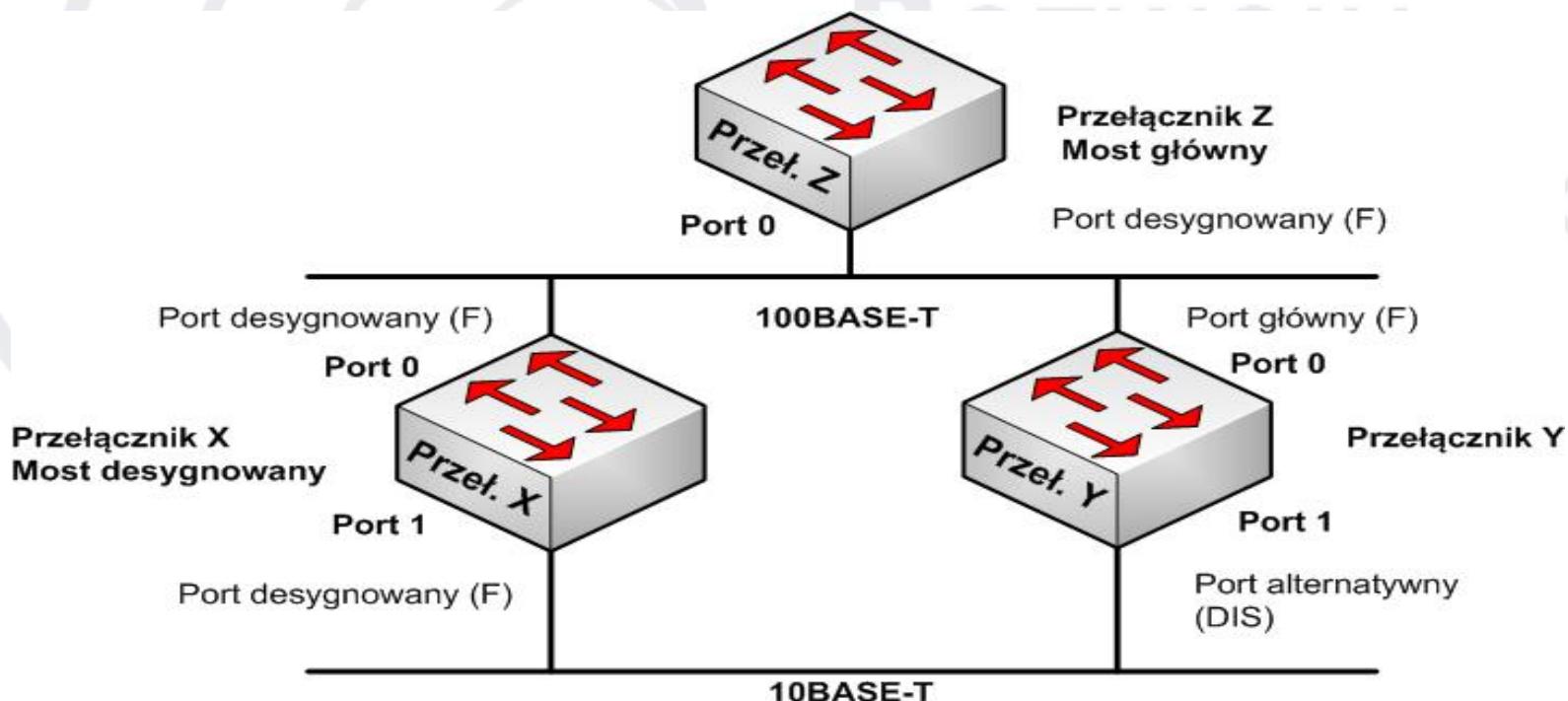
# Ponowne obliczanie drzewa



- Przy zmianie topologii sieci przełączniki muszą ponownie wykonać obliczenia protokołu STP (zakłóca to ruch użytkowników)
- Porty przekazujące wysyłają i odbierają dane i jednostki BPDU, a porty blokujące jedynie odbierają jednostki BPDU

# Protokół RSTP

- Szybki Protokół STP – **RSTP** (*Rapid Spanning Tree Protocol*) znaczowo skraca czas realizacji zbieżności w aktywnej topologii sieci po zmianach topologii fizycznej lub modyfikacji parametrów sieci

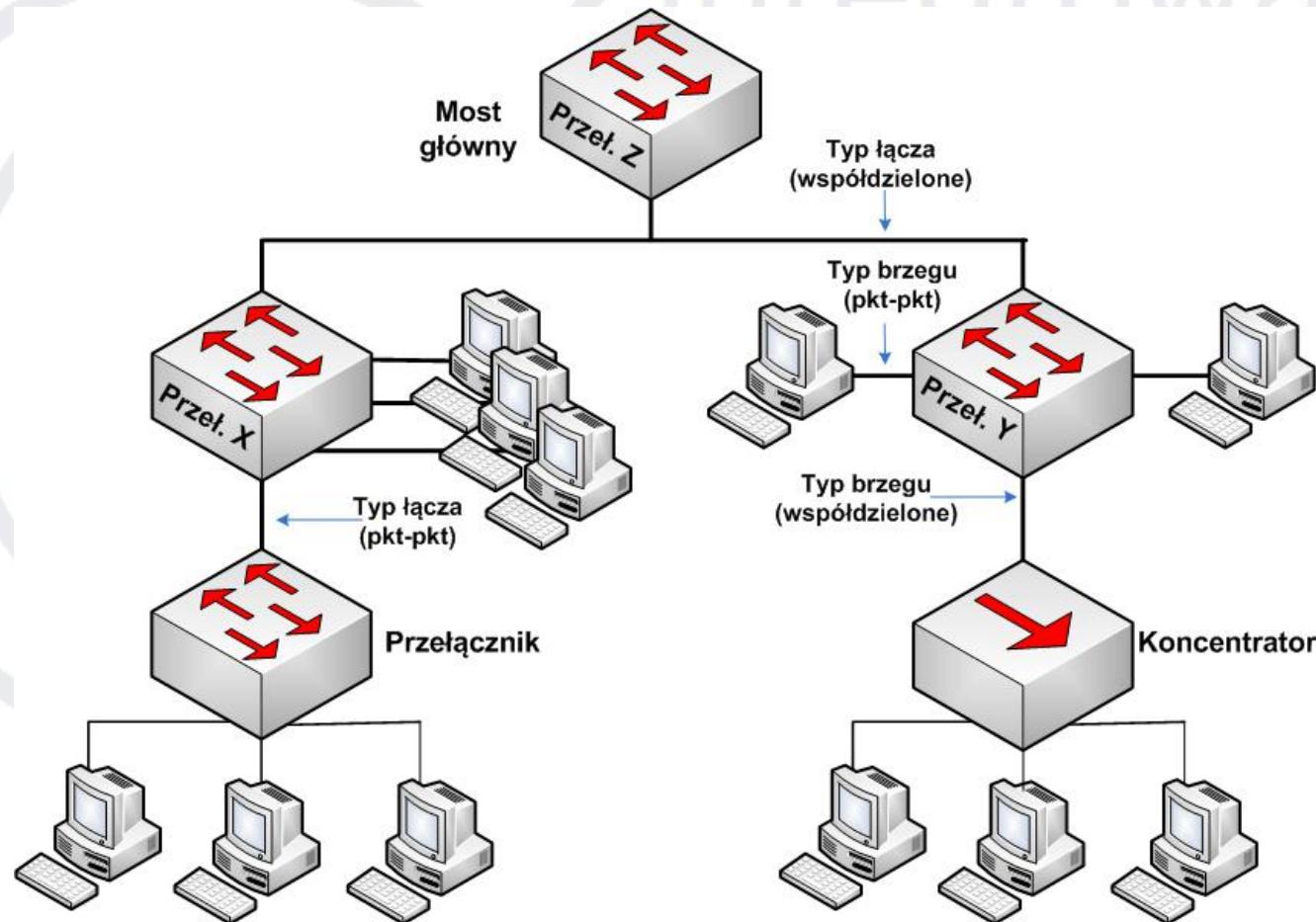


# Protokół RSTP

- Port **główny i desygnowany** biorą czynny udział w aktywnej topologii, natomiast **alternatywny i zapasowy** są z niej wyłączone
- W stabilnej topologii, RSTP gwarantuje, że każdy port główny i desygnowany przechodzi do przekazywania, a wszystkie porty alternatywne i zapasowe są w stanie odrzucania

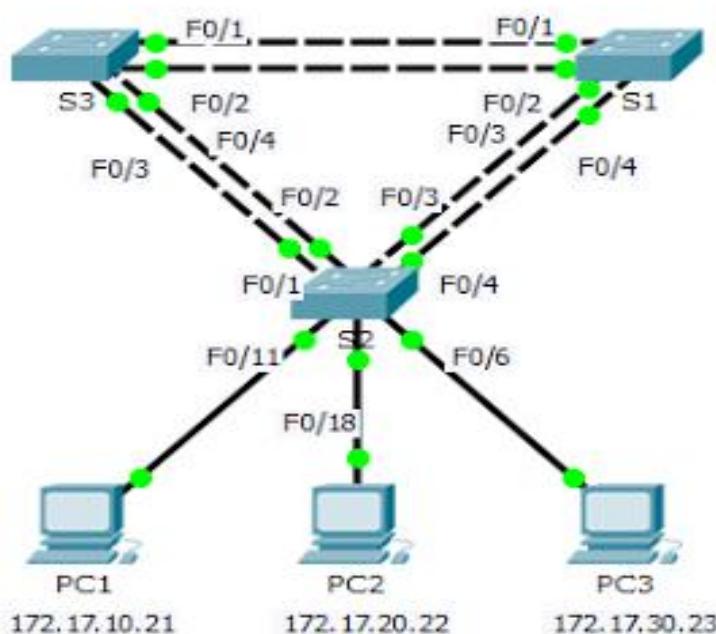
Stan operacyjny	Stan portu STP	Stan portu RSTP	Udział portu w aktywnej topologii
Włączony	Blokowanie	Odrzucanie	Nie
Włączony	Nasłuchiwanie	Odrzucanie	Nie
Włączony	Uczenie się	Uczenie się	Tak
Włączony	Przekazywanie	Przekazywanie	Tak
Wyłączony	Wyłączenie	Odrzucanie	Nie

# Porty brzegowe i łącza p2p



# STP - Cisco Rapid-PVST+

- Protokół PVST+ (ang. Per-VLAN Spanning Tree +) , opracowany przez Cisco protokół, którego zadaniem jest tworzenie osobnych instancji drzewa rozpinającego dla każdej z wykorzystywanych sieci VLAN



Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.12
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.12
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.12

Źródło rysunku: Configuring RAPID PVST+, <http://projekkuliah.blogspot.com/2018/10/configuring-rapid-pvst.html>

# Techniki łączenia przełączników

- Wybór przełączników przeprowadzany jest na etapie projektowania sieci LAN
- Jakie urządzenia i o jakiej gęstości portów (12, 24, 48)
- praktycznie rzadko zdarza się, że urządzenie ma wystarczającą ilość portów (a jeśli nawet to sieci raczej się rozrastają)
- Dodanie nowych stacji nie może wiązać się z przeprojektowaniem sieci!
  - 10 stacji => urządzenie 24-portowe
  - 36 stacji => 2 x urządzenia 24-portowe lub 1 x 48-portowe
- Połączenia port-port
- Agregacja łączy

# Połączenia port-port

## Zalety

- Niski koszt realizacji
- Łatwość rozbudowy

## Wady

- Relatywnie niewielka wydajność
- Mała skalowalność
- Brak redundantności

Przełącznik X



Przełącznik Y



Przełącznik Z



# Agregacja łączy

- Z reguły, aby konfiguracja agregacji na parze przełączników przebiegła pomyślnie, należy na obu urządzeniach:
  - wybrać do agregacji taką samą ilość i typ portów (typu medium, skonfigurowana prędkość, tryb pracy)
  - wybrać nie więcej niż 8 portów (ograniczenie 802.3ad, lub producenta)
  - w przypadku przełączników różnych producentów, należy skonfigurować na obu ten sam standard agregacji (IEEE 802.3ad) i ewentualnie odpowiedni protokół kontroli tak utworzonej agregacji (firmowy **Cisco PAgP** lub **IEEE LACP**)
  - w produktach niektórych producentów tak stworzoną agregację należy jeszcze dodatkowo uaktywnić

Przełącznik X



Przełącznik Y



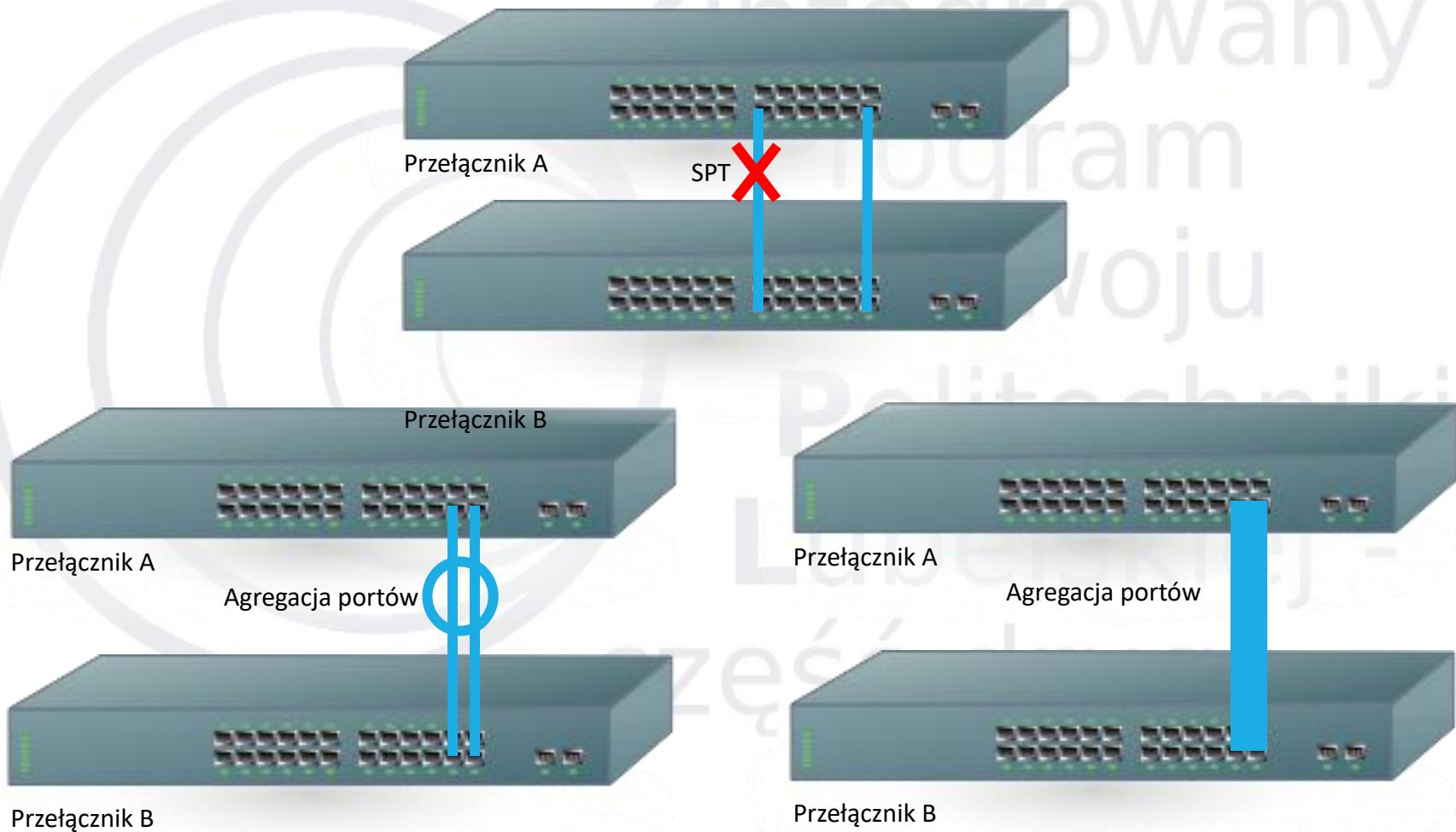
Przełącznik Z



Agregacja 2 portów

Agregacja 2 portów

# Agregacja łączy



**POLITECHNIKA LUBELSKA**

**WYDZIAŁ ELEKTROTECHNIKI I INFORMATYKI**

**INFORMATYKA**



Zintegrowany  
Program  
Rozwoju  
Politechniki  
Lubelskiej -  
część druga

## Podstawy Sieci Komputerowych

### Rodzina standardów IEEE 802.1 i IEEE 802.3 Sieci bezprzewodowe

dr hab. inż. Konrad Gromaszek



**Fundusze  
Europejskie**  
Wiedza Edukacja Rozwój



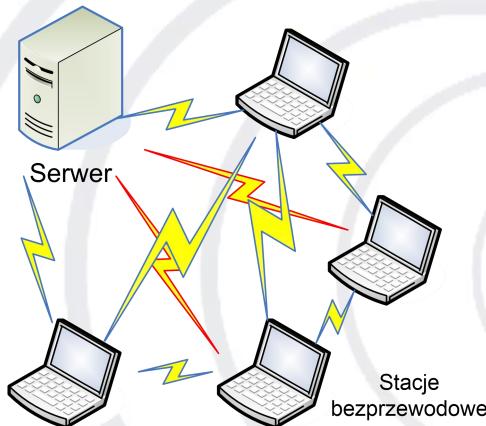
**Rzeczpospolita  
Polska**

**Unia Europejska**  
Europejski Fundusz Społeczny



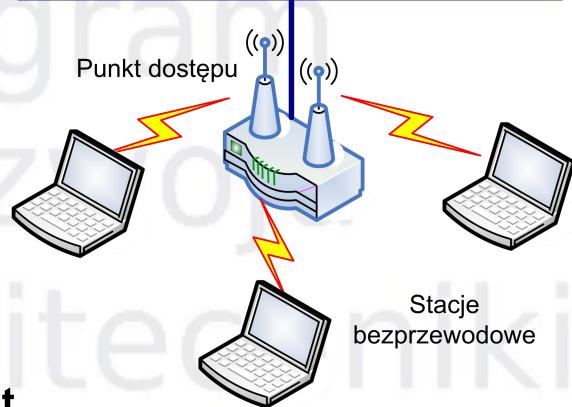
# Standard IEEE 802.11

## IBSS – Independent Basic Service Set



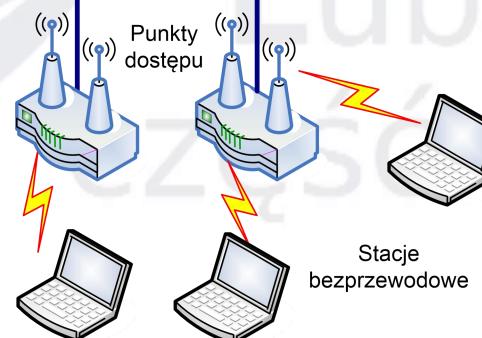
## BSS – Basic Service Set

Przewodowa sieć LAN



## ESS – Extended Service Set

Przewodowa sieć LAN

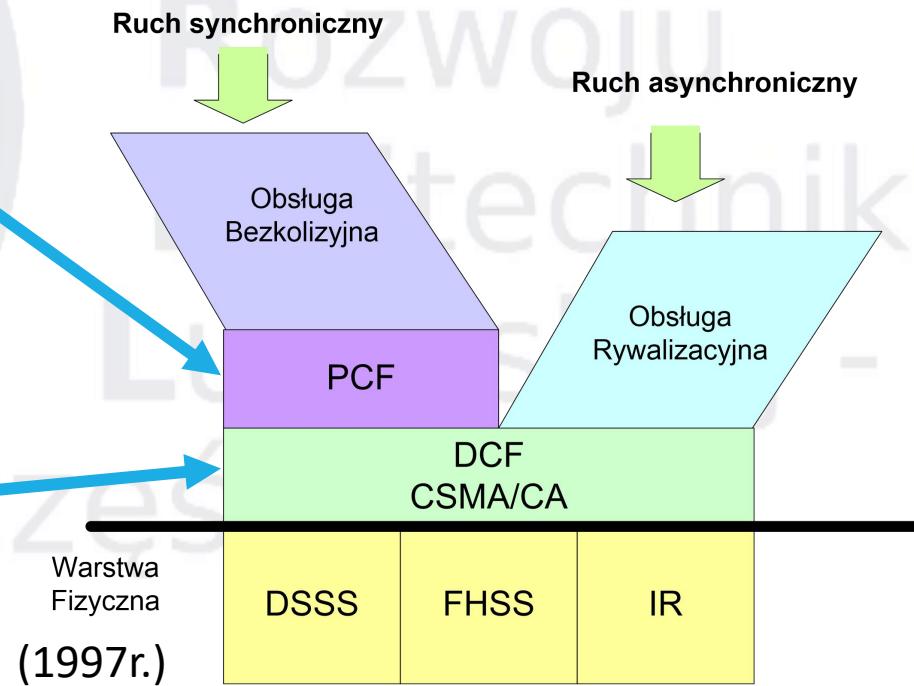


# IEEE 802.11 - dostęp do medium

- W standardzie IEEE 802.11 podwarstwa dostępu do łącza jest niezależna od sposobu realizacji warstwy fizycznej

**PCF** - tryb z punktową funkcją koordynacji, przeznaczony dla sieci stałych, wyposażonych w AP

**DCF** - tryb z rozproszoną funkcją koordynacji (algorytm podstawowy)



# Warstwa fizyczna 802.11 (legacy)

- Standard 802.11 z 1997 roku definiuje trzy techniki dopuszczalne w warstwie fizycznej:
  - Metoda na podczerwień
  - FHSS (ISM 2,4Ghz)
  - DSSS (ISM 2,4Ghz)
- W roku 1999 wprowadzono:
  - OFDM
  - HR-DSSS
- W roku 2001
  - Druga OFDM



# Warstwa fizyczna 802.11 (do 2019)

	PHY	Protocol	Release	Freq	Band	Stream data rate	Mimo	Modulation
1-6 GHz	DSSS/FHSS	802.11-1997	06.1997	2,4	22	1, 2	N	DSSS, FHSS
	HR-DSSS	802.11b	09.1999	2,4	22	1, 2, 5,5, 11	N	DSSS
	OFDM	802.11a	09.1999	5	5 / 10 / 20	6, 9, 12, 18, 24, 36, 48, 54	N	OFDM
		802.11j	11.2004	4,9/5				
		802.11p	07.2010	5,9				
		802.11y	11.2008	3,7				
	ERP-OFDM	802.11g	06.2003	2,4				
	HT-OFDM	802.11n	10.2009	2,4/5	20/40	288,8 600	4	MIMO-OFDM
	VHT-OFDM	802.11ac	12.2013	5	20-160	346,8-3466,8	8	MIMO-OFDM
	HE-OFDM	802.11ax	09.2019	2,4/5/6	20-80	1147-10530	8	MIMO-OFDM

# Warstwa fizyczna 802.11 (do 2019)

	PHY	Protocol	Release	Freq	Band	Stream data rate	Mimo	Modulation
mmWave	DMG	802.11ad	12.2012	2,4	2, 160	6,7 Gbps	N	OFDM, single carrier, low power
		802.11aj	04.2018	2,4	540/1080	15 Gbps	4	OFDM, single carrier
	EDMG	802.11ay	05.2020		8000	20 Gbps	4	OFDM, single carrier
Sub-1 GHz IoT	TVHT	802.11af	02.2014	0,054-0,079	6-8	568,9		MIMO-OFDM
	S1G	802.11ah	12.2016	0,7/0,8/0,9	1-16	8,67	4	MIMO-OFDM
2,4GHz, %GHz	WUR	802.11ba	09.2020	2,4/5	4,06	62.5 kbit/s, 250 kbit/s		
Light	IR	802.11ac	06.1997	?	20-160	1, 2	N	PPM
	?	802.11ax	07.2021	60k-79k	20-80	?	N	?

# Warstwa fizyczna 802.11 - OFDM

- **OFDM (*Orthogonal Frequency Division Multiplexing*)** – multipleksowanie z ortogonalnym podziałem częstotliwości
  - Wykorzystywana w pierwszej z szybkich bezprzewodowych sieci lokalnych **IEEE 802.11a**
  - Pozwalała na szybkość 54Mb/s w szerszym **paśmie 5 GHz**
  - Używa 52 różne częstotliwości (48 dla danych i 4 dla synchronizacji)
  - Uznawana za formę widma rozproszonego
  - Większa odporność na zakłócenia wąskopasmowe oraz możliwość korzystania z pasm ciągłych dzięki podziałowi na wiele wąskich pasm
  - stosuje system kodowania oparty na modulacji fazy dla szybkości do 18 Mb/s i QAM powyżej
  - Przy 54 Mb/s 216 bitów danych jest kodowanych do 288-bitowych symboli
- OFDM jest zgodna z europejskim systemem HiperLAN/2
- Zapewnia dobre wykorzystanie pasma (mierzone w b/Hz) i dobrą odporność na wielodrożne zaniki sygnału

# W. fizyczna 802.11 – OFDM 2

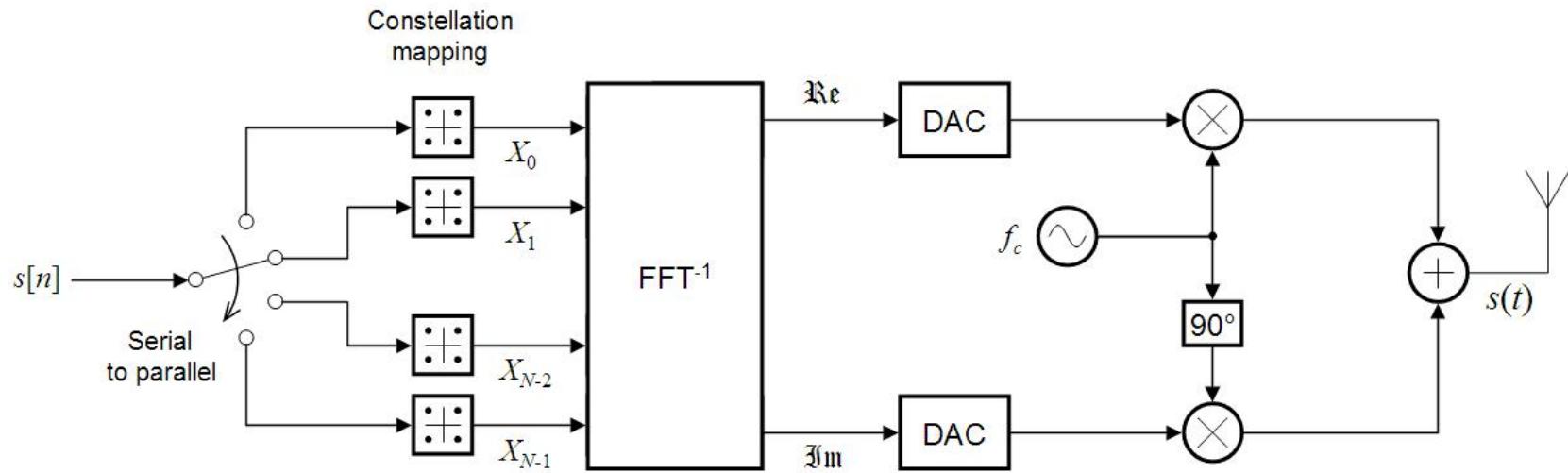
- **OFDM (*Orthogonal Frequency Division Multiplexing*)** – multipleksowanie z ortogonalnym podziałem częstotliwości

Zalety	Wady
<ul style="list-style-type: none"><li>• Efektywne wykorzystanie pasma</li><li>• Możliwa kontrola stanu kanału radiowego i dostosowanie do niego parametrów odbioru</li><li>• Dobrze radzi sobie z interferencjami międzysymbolowymi i zanikami</li><li>• Zmniejszona wrażliwość na niedokładność synchronizacji</li><li>• Nie wymaga przestrjalnych filtrów w odbiornikach podkanałów (w przeciwieństwie do trad. FDM)</li></ul>	<ul style="list-style-type: none"><li>• Wrażliwość na problemy z synchronizacją częstotliwości nośnej</li><li>• Niekorzystny kształt widma mocy, wymagający użycia liniowego toru nadawczo-odbiorczego</li><li>• Obniżona efektywność transmisji wynikająca z zastosowania cyklicznego prefiksu i okresu ochronnego</li><li>• Wrażliwość na efekt Dopplera</li></ul>

# OFDM – model systemu

- Nadajnik

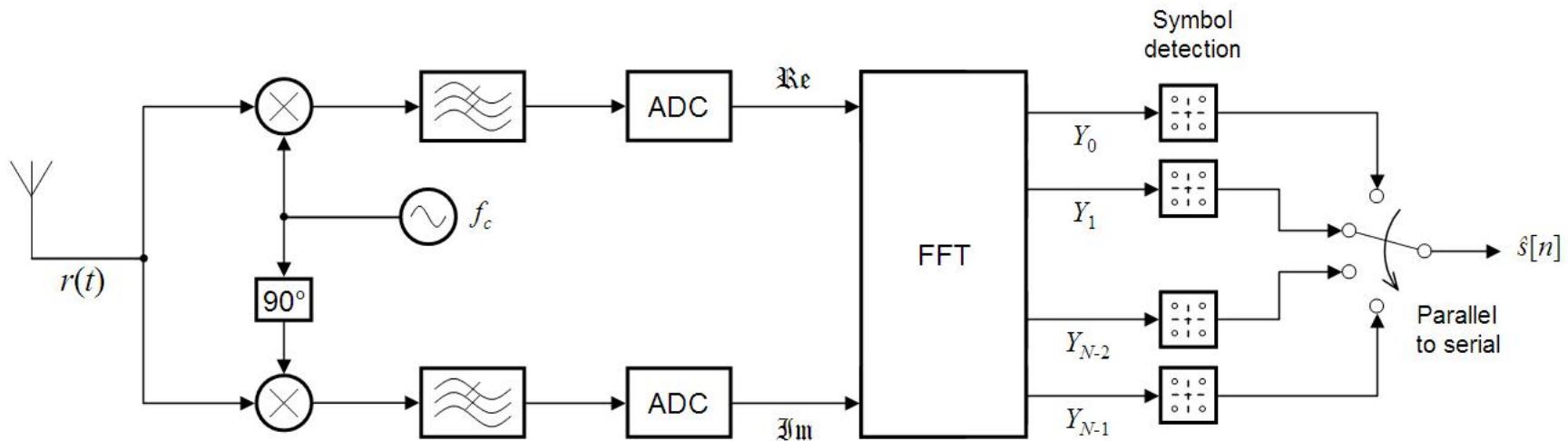
- Sygnał nośny w OFDM jest sumą ortogonalnych nośnych podkanałów, gdzie w każdym z nich występuje kwadraturową modulacją amplitudy (QAM) lub kluczowanie fazy (PSK)



Źródło rysunku: Oli Filth, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=1816416>

# OFDM – model systemu

- Odbiornik odbiera sygnał  $r(t)$ 
  - Poza sygnałem użytecznym powstaje również sygnał o częstotliwości  $2 f_c$
  - Do jego odfiltrowania stosuje się filtr dolnoprzepustowy
  - Następnie, sygnał jest próbkowany i podawany na przetwornik AC
  - Dalej wykonywana jest FFT i detekcja symboli
  - $N$  równoległych strumieni łączy się w jeden, uzyskując pierwotny ciąg bitów

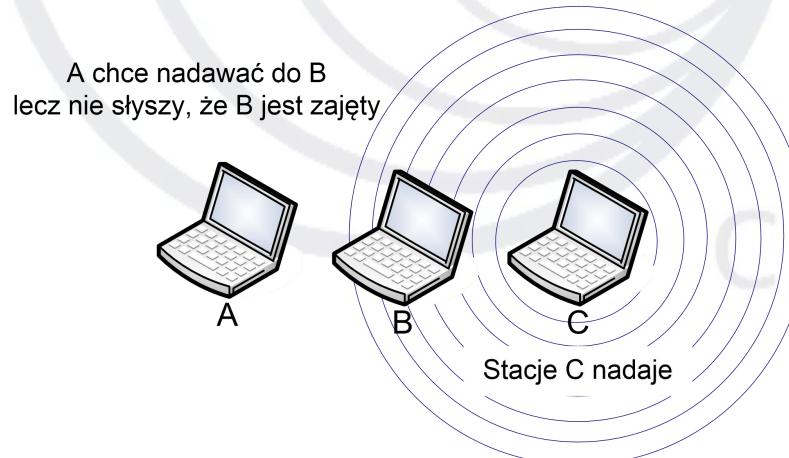


Źródło rysunku: Oli Filth, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=1816465>

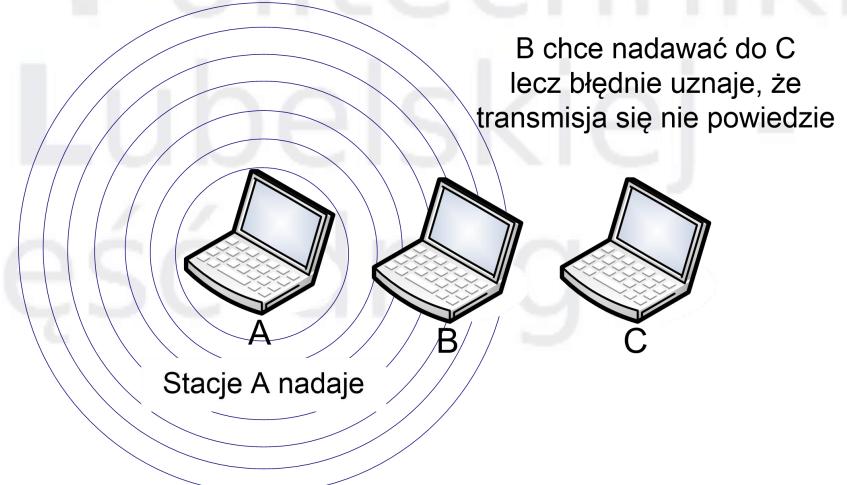
# Protokół warstwy MAC w 802.11

- Różny od odpowiednika z Ethernetu (ze względu na złożoność środowiska bezprzewodowego)
- Nie wszystkie stacje znajdują się w zasięgu pozostałych, zatem transmisje odbywające się w jednym miejscu komórki mogą nie zostać odebrane w innym miejscu tej samej komórki:

**Problem ukrytej stacji**



**Problem odkrytej stacji**

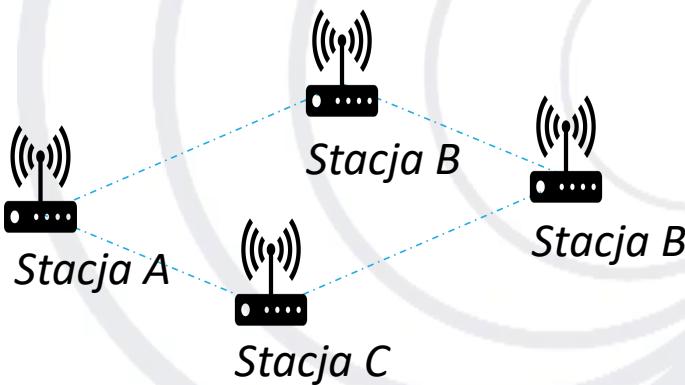


# IEEE 802.11 - DCF

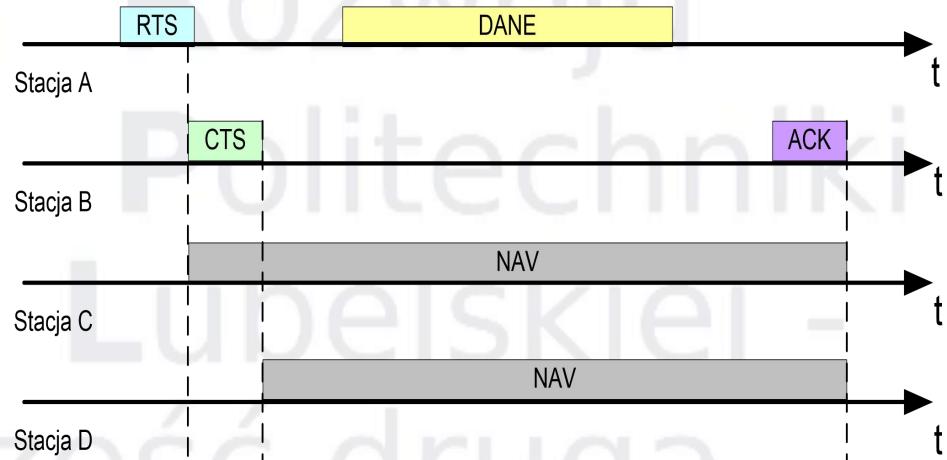
- W trybie DCF, 802.11 używa protokołu **CSMA/CA** (**CSMA *witch Collision Avoidance***), w którym używane jest wyrywanie kanału fizycznego i wirtualnego. Pozwala na dwa tryby działania:
- **Tryb I** – stacja, która chce nadawać sprawdza stan nośnika; nadaje,
  - wykrywając wolny kanał (bez sprawdzania stanu kanału podczas nadawania); wówczas ramka może dotrzeć do odbiornika zniszczona;
  - w przypadku zajętości kanału czeka na jego zwolnienie, po czym zaczyna nadawać; w razie kolizji, obydwie stacje (N+O) odczekują losowy czas i ponawiają próbę
- **Tryb II** - opiera się na MACAW i stosuje wykrywanie kanału wirtualnego

# IEEE 802.11 - DCF

- CSMA/CA Tryb II - Przykład: Stacja A chce nadać do B, a C jest stacją w zasięgu A. D jest stacją w zasięgu B, ale poza zasięgiem A



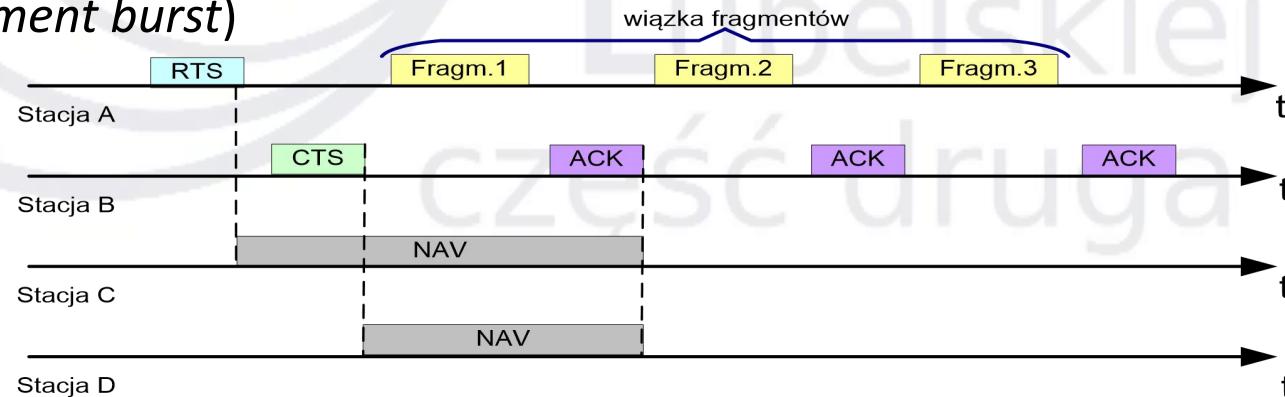
Wykrywanie kanału wirtualnego z użyciem CSMA/CA



- NAV – Network Allocation Vector – oznaczenie zajętości kanału / powstrzymanie od transmisji przez stacje ościenne, aż do zakończenia wymiany danych

# IEEE 802.11 – DCF a zakłócenia

- W sieciach bezprzewodowych występuje znaczny wpływ zakłóceń, zatem szansa pomyślnego dotarcia ramki do celu maleje wraz z długością ramki
- Prawdopodobieństwo bezbłędnego odebrania  $n$ -bitowej ramki wynosi  $(1-p)^n$ , gdzie  $p$  – prawdopodobieństwo wystąpienia błędu w określonym bicie (dla  $p=10^{-5}$  jedna ramka na 9 dotrze uszkodzona)
- Problem zakłóceń w kanale 802.11 niweluje się podziałem ramek na mniejsze fragmenty
- Sekwencja fragmentów, określana jest wiązką fragmentów (*fragment burst*)

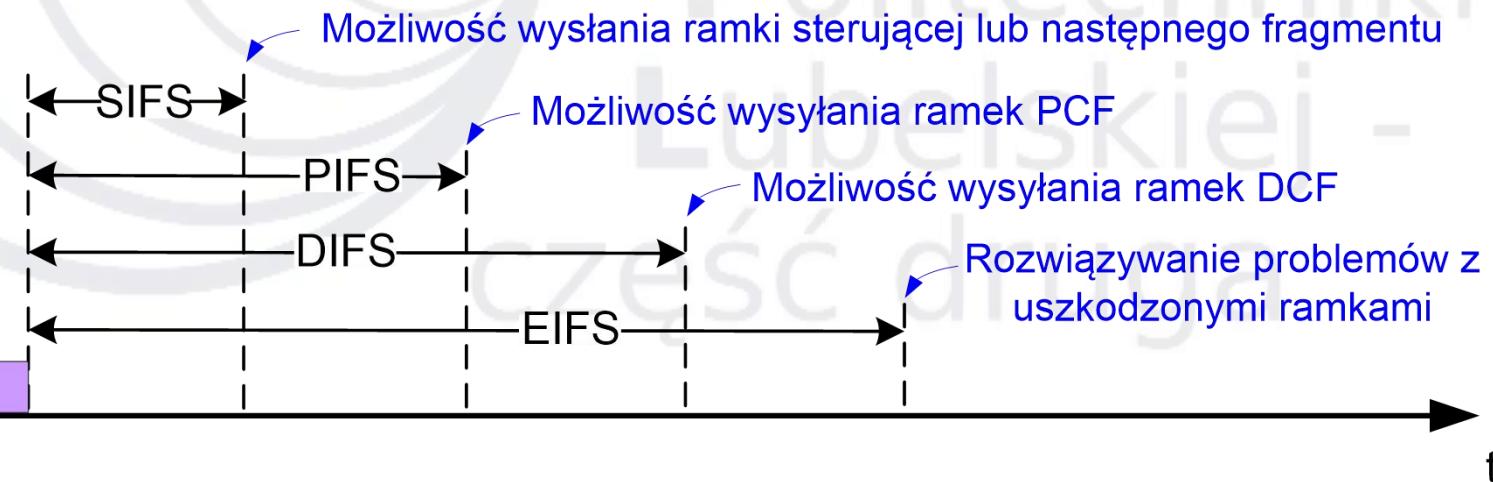


# IEEE 802.11 - PCF

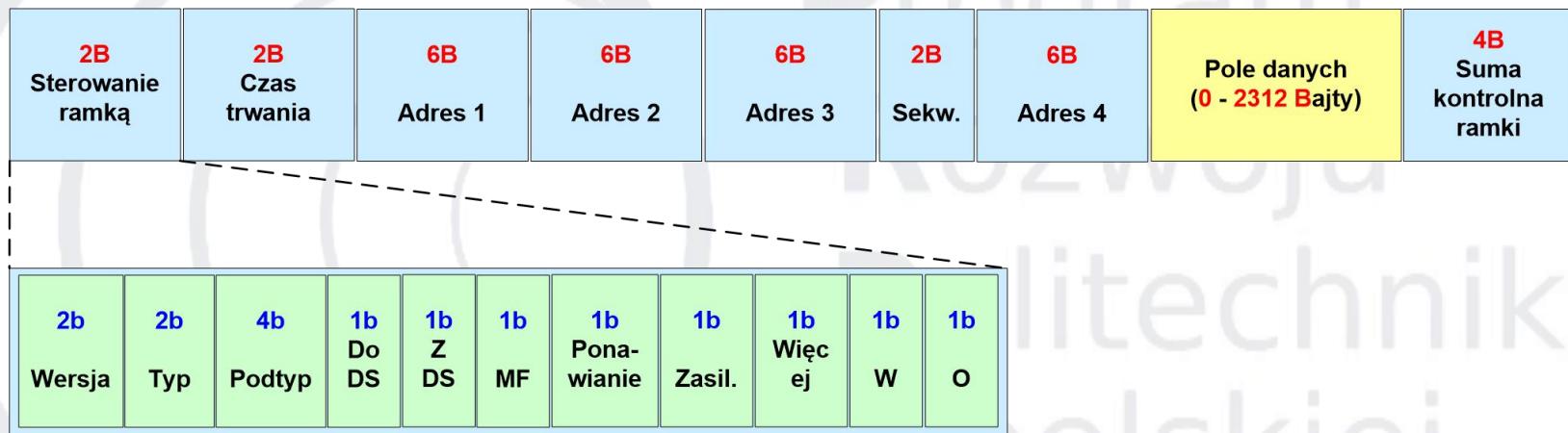
- Kolejność transmisji kontrolowana przez stację bazową = brak kolizji
- podstawowy mechanizm polega na okresowym rozgłaszeniu przez stację bazową ramki nawigacyjnej, zawierającej parametry systemu, która zaprasza nowe stacje do zapisywania się na usługę odpytywania
- Po zapisaniu się stacji na usługę odpytywania z określona częstotliwością , ma ona zagwarantowaną część pasma, co pozwala gwarantowanie QoS
- W kwestii oszczędności energii, stacja bazowa może wprowadzić stację mobilną w tryb uśpienia do czasu wybudzenia przez stację bazową lub użytkownika; do tego czasu stacja bazowa buforuje wszelkie ramki kierowane do stacji mobilnej

# Współistnienie PCF i DCF

- Jednoczesne sterowanie centralne i rozproszone jest realizowane poprzez dokładne zdefiniowanie **odstępów czasu** między ramkami
- Po wysłaniu ramki wymagany jest określony czas martwy, zanim którakolwiek stacja będzie wysyłać ramkę
- Standard 802.11 definiuje cztery interwały:



# Struktura ramki IEEE 802.11



# IEEE 802.11n

- **IEEE 802.11n** należy do grupy standardów IEEE dla WLAN
- zatwierdzony w roku 2010 ( w 2004 - urządzenia 100-300Mb/s)
- pracuje z szybkościami 100,35; 252,88; 540 Mb/s przy pasmie częstotliwości 2.4 lub 5.0 GHz
- Stosuje technologię **Multiple Input Multiple Output (MIMO)** wykorzystująca wiele anten do nadawania/odbioru sygnału (jest nadawany z kilku źródeł i odbierany przez kilka odbiorników)
- Urządzenia 802.11n potrafią wykorzystywać wiele kanałów transmisyjnych do stworzenia jednego połączenia, co teoretycznie dodatkowo podwaja dostępną prędkość transmisji
- Przepustowość sieci 802.11n sięga do 600 Mb/s

# IEEE 802.11ac

- Rozwiązanie MIMO zostało przeniesione do specyfikacji **802.11ac**, która wprowadziła dodatkowo zaawansowane techniki modulacji w postaci 256 QAM
- Wave1: łącze o fizycznej maksymalnej prędkości 433 Mb/s, w ramach jednego strumienia, typowo  $3 \times 433\text{Mb/s} = 1,3\text{Gbs}$
- Wave2: (2015 r.) większa szerokość kanałów na częstotliwości 5GHz oraz nową technikę DL **MU-MIMO** (*Downlink multiuser multiple input / multiple output*), wydajność każdego strumienia została zwiększona
- Faza druga 802.11ac wspiera nawet do ośmiu strumieni MIMO (zgodnie z aktualnymi założeniami specyfikacji 4)
- Wykorzystanie kombinacji tych technologii, dostarcza maksymalną prędkość łączego bezprzewodowego na poziomie 7-10 Gb/s

# IEEE 802.11ax

- Specyfikacja **802.11ax** jest bliska 802.11ac Wave2, ale zawiera pewne elementy rewolucyjne z punktu widzenia Wi-Fi
- wykorzystuje wyłącznie częstotliwość 5GHz z szerokością kanału 80MHz lub 160MHz
- Podobnie jak w 802.11ac Wave2 wykorzystywanych będzie maksymalnie osiem strumieni MIMO, każdy strumień wysyłany przy wykorzystaniu techniki OFDMA (*Orthogonal Frequency Division Multiple Access*)
- Specyfikacja 802.11ac zakłada wykorzystywanie technologii Downlink MU-MIMO w kierunku DL (Downlink) do klienta
- W przypadku 802.11ax wspierana będzie także technologia Uplink MU-MIMO w kierunku UL (Uplink) od klienta

# Sieci kratowe standardu 802.11s

- **IEEE 802.11s** - zatwierdzony w 2011 standard, określający działanie bezprzewodowych sieci komputerowych o topologii kratowej (ang. *Mesh Topology Network*) i współpracę takiej sieci z innymi sieciami zgodnymi z IEEE 802.11
- Założeniem topologii mesh jest możliwość komunikacji pomiędzy elementami sieci bez konieczności angażowania jednostki AP
- W takiej sieci każde urządzenie sieciowe może komunikować się z każdym innym urządzeniem bezpośrednio (warunek sąsiedztwa) lub za pośrednictwem dowolnych innych elementów sieci (gdy element docelowy jest poza bezpośredniem zasięgiem źródła)

# Routing w IEEE 802.11s

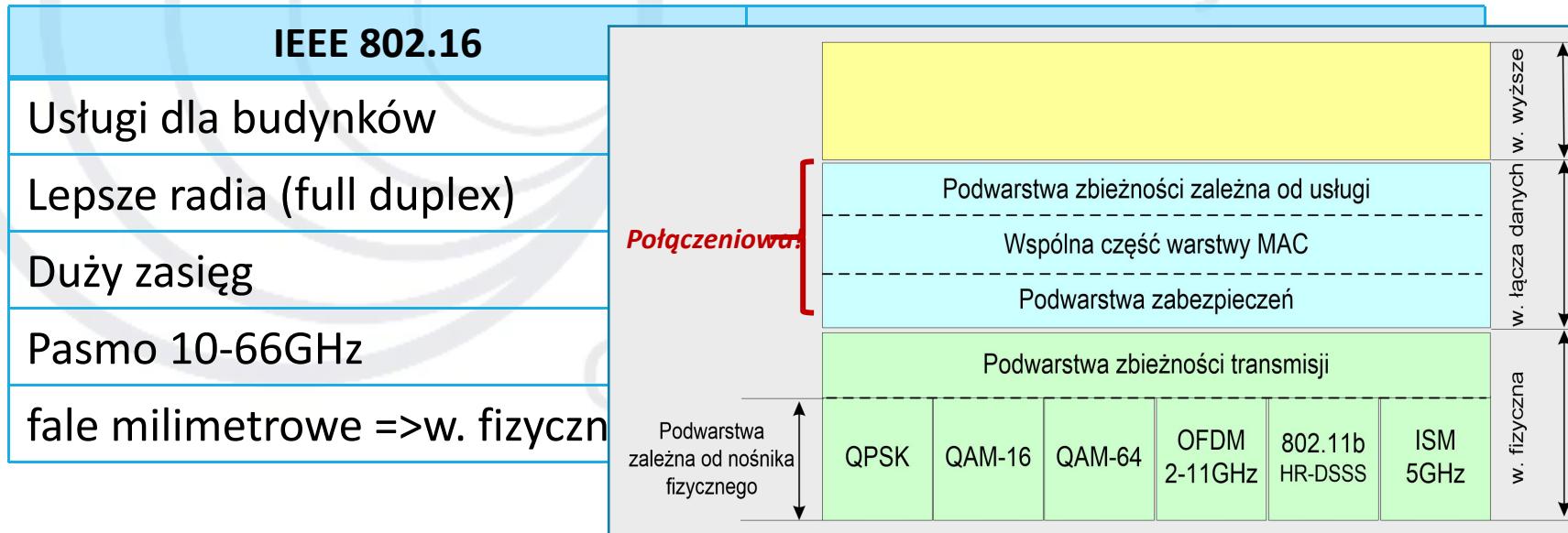
- Głównym założeniem trasowania sieci mesh jest kompatybilność z innymi sieciami zgodnymi z 802.11
- Trasowanie zdefiniowane w 802.11s opiera się na 2 protokołach:
  - **Domyślny – HWMP** (ang. *Hybrid Wireless Mesh Protocol*) – łączy dynamiczny sposób trasowania ***on-demand***(RM-AODV, RFC 3561) i polega na wyszukiwaniu drogi poprzez rozsyłanie pakietów „Route Request”) i metodę ***pro-active tree*** (oparta na zasadzie struktury drzewa).
  - **Opcjonalny – RA-OLSR** (ang. *Radio Aware Optimized Link State Routing protocol*) – oparty na protokole OLSR (ang. Optimized Link State Routing, RFC 3626), który został poszerzony o protokoły współpracujące z sieciami zgodnymi z 802.11

# Sieci kratowe standardu 802.11s

Zalety	Wady
<ul style="list-style-type: none"><li>minimalizacja nakładów na infrastrukturę</li><li>możliwość dowolnego zwiększenia obszaru zasięgu</li><li>istnienie alternatywnych dróg transmisji</li><li>adaptacyjne dostosowywanie do warunków, odporność na ataki fizyczne</li><li>możliwość uzyskanie zasięgu NLOS (dodatkowy węzeł do omijenia przeszkody)</li></ul>	<ul style="list-style-type: none"><li>zwiększone opóźnienie (wiele skoków),</li><li>może być nie tolerowane przez niektóre aplikacje wymagające transmisji w czasie rzeczywistym</li><li>skomplikowanie protokołów sieciowych (dodatkowe funkcje w definiowaniu dostępu do sieci i wyboru trasy - routing),</li><li>złożoność planowania pokrycia</li></ul>

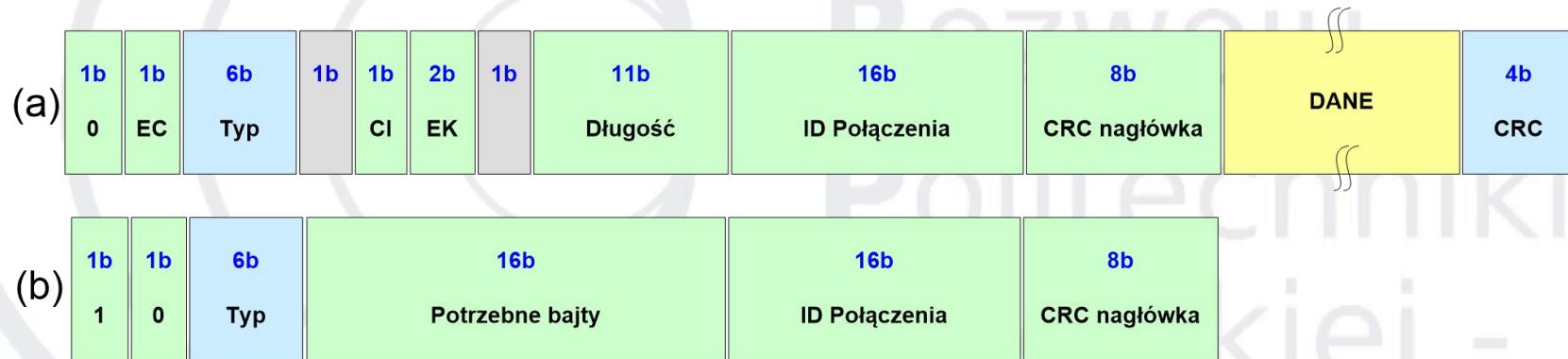
# Szerokopasmowe łącza bezprzewodowe

- Czerwiec 1999 – wszczęcie prac nad standardem **802.16**, ostatecznie zaaprobowanym w kwietniu 2002, którego oficjalna nazwa brzmi: **Air Interface for Fixed Broadband Wireless Access Systems**, lecz niektórzy określają go **Wireless MAN** lub **wireless local loop**



# Struktura ramki IEEE 802.16

- Standardowy format ramki (a)
- Ramka z żądaniem pasma (b)



- EC – czy zaszyfrowany ładunek ramki
- EK – używany klucz szyfrujący
- CI – wskazuje obecność/brak sumy kontrolnej

# IEEE 802.16d/e - WiMAX

- **WiMAX (*Worldwide Interoperability for Microwave Access*)** – technika bezprzewodowej, radiowej transmisji danych, oparta na standardach IEEE 802.16 i ETSI HiperLAN w celu realizacji szerokopasmowego, radiowego dostępu na dużych obszarach
- WiMAX 802.16e jest technologią, która w głównym zamyśle pozwala na zapewnienie dostępu do Internetu w urządzeniach stacjonarnych i mobilnych, jako alternatywa świadczenia tej usługi w sposób przewodowy
- Od 2009 roku największe światowe sieci komórkowe rezygnują z tej techniki na rzecz stopniowej migracji do sieci standardu LTE

# Bluetooth i IEEE 802.15.1

- W 1994 Podstawową jednostką Bluetooth jest **piconet**, która składa się z **węzła głównego** (master) i maksymalnie 7 aktywnych **węzłów podrzędnych** (slave) w odległości do 10 m
- W pomieszczeniu może pracować kilka piconet'ów, można je łączyć węzłem mostu, tworząc **scatternet**
- Poza aktywnymi węzłami podrzędnymi w sieci piconet może znajdować się do 255 **węzłów zaparkowanych**, czyli urządzeń wprowadzonych przez węzeł główny w stan niskiego poboru energii, (węzeł tego rodzaju oczekuje na sygnał aktywacji lub nawigacyjny od węzła głównego)
- Piconet jest w zasadzie zcentralizowanym systemem TDM, w którym węzeł główny kontroluje zegar i przydziela szczeliny czasowe urządzeniom
- Komunikacja między dwoma węzłami podrzędnymi jest niemożliwa

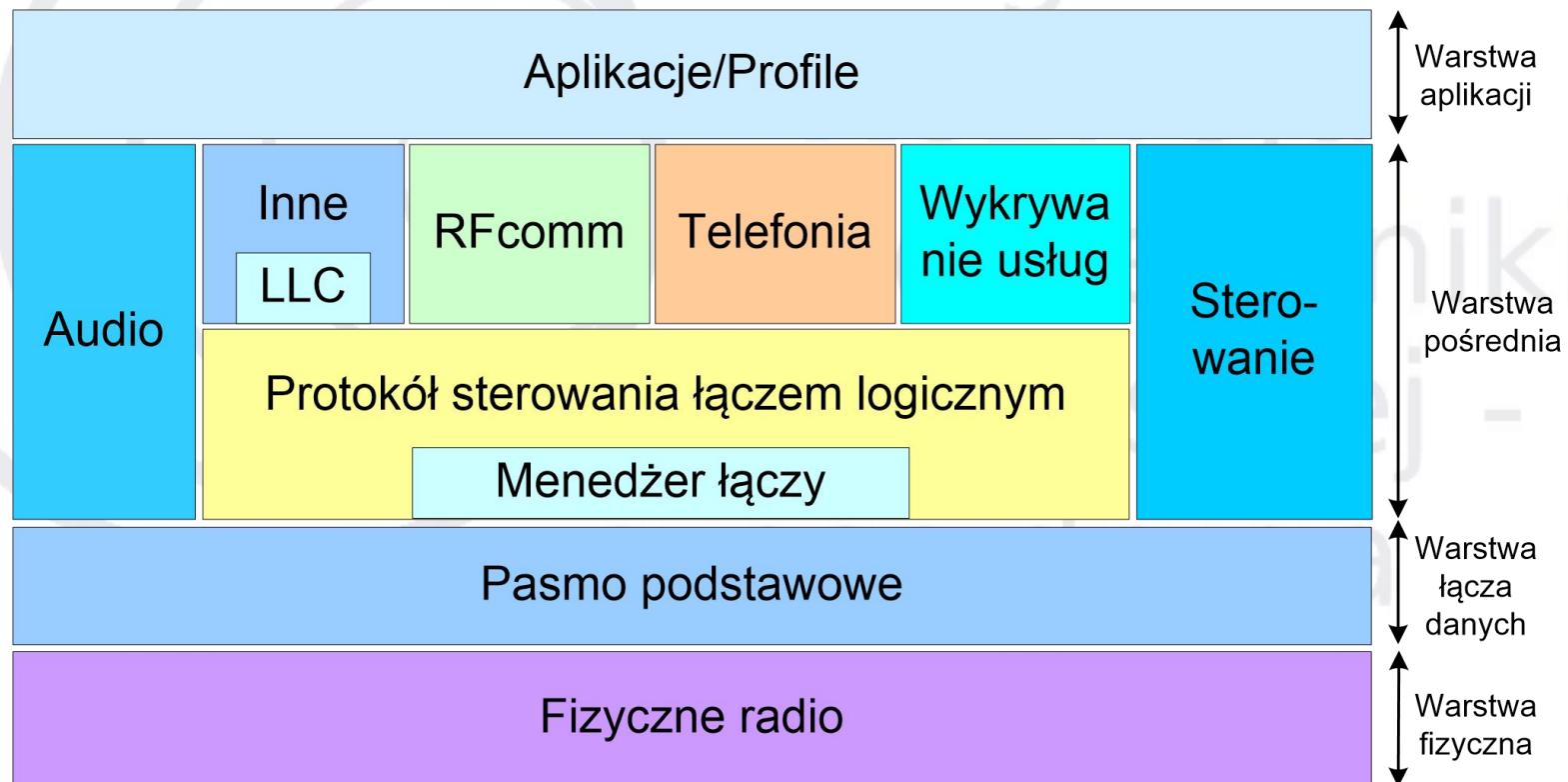
# Profile Bluetooth

- Większość protokołów sieciowych określa kanały pomiędzy komunikującymi się jednostkami i pozwala projektantom aplikacji na dowolne ich użycie
- Wersja 1.1 Bluetooth określa 13 specjalnych aplikacji, tzw. profili systemu Bluetooth

Nazwa	Opis
Generic access	Procedury zarządzania łączem
Service discovery	Protokół do wykrywania oferowanych usług
Serial port	Alternatywa kabla szeregowego
Generic object exchange	Definiuje relacje klient-serwer dla przenoszenia obiektów
LAN access	Protokół pomiędzy hostem mobilnym i stacjonarną LAN
Dial-up networking	Łączenie hosta przez np. telefon komórkowy
Fax	Łączenie się przenośnego faksu przez tel. komórkowy
Cordless telephony	Łączy zestaw słuchawkowy z lokalną stacją bazową
Intercom	Cyfrowe walakie-talkie
Headset	Obsługa zestawów słuchawkowych
Object push	Udostępnia sposób wymiany obiektów
File transfer	Przesyłanie plików
Synchronization	Umożliwia synchronizację np. PDA z innym hostem

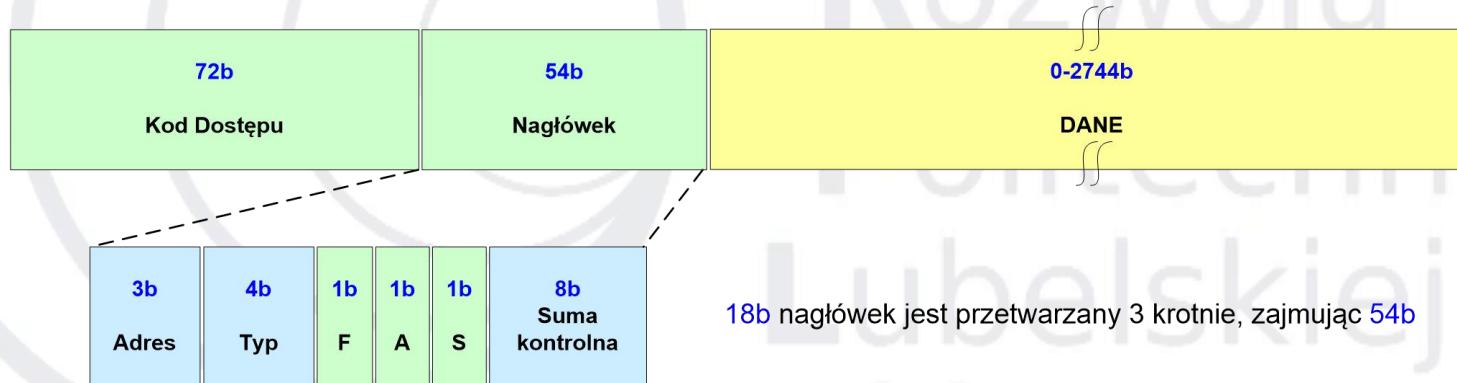
# Stos protokołów Bluetooth

- Struktura warstw BT nie jest zgodna z modelami OSI, TCP/IP, 802, ani żadnym innym!



# Ramka Bluetooth

- Istnieje kilka formatów ramki w systemie Bluetooth, jednak najważniejszą i najczęściej stosowaną jest ta przedstawiona na rysunku.



# Elementy urządzenia Bluetooth

- Większość procesów realizowanych przez pasmo podstawowe oparte jest na dwóch elementach urządzenia Bluetooth, obejmujących:
  - **adres urządzenia Bluetooth**
    - *Bluetooth Device Address* - adres urządzenia Bluetooth
    - *Active Member Address* - adres urządzenia aktywnego
    - *Parked Member Address* - adres zaparkowanego elementu pikosieci
    - *Access Request Address* - adres żądania przyłączenia
  - **zegar urządzenia Bluetooth (28b)**
    - determinuje synchronizację i skakanie po częstotliwościach
    - do synchronizacji z innym modelem Bluetooth wykorzystywana jest różnica (offset) pomiędzy zegarami jednostek biorących udział w komunikacji
    - częstotliwość zegara wynosi 3,2 kHz,  $\Omega = 24\text{h}$



## Podstawy Sieci Komputerowych

## Charakterystyka warstwy sieciowej. Podstawy doboru trasy w sieciach IP cz.1

dr hab. inż. Konrad Gromaszek



**Fundusze  
Europejskie**  
Wiedza Edukacja Rozwój



**Rzeczpospolita  
Polska**

**Unia Europejska**  
Europejski Fundusz Społeczny



# Wprowadzenie

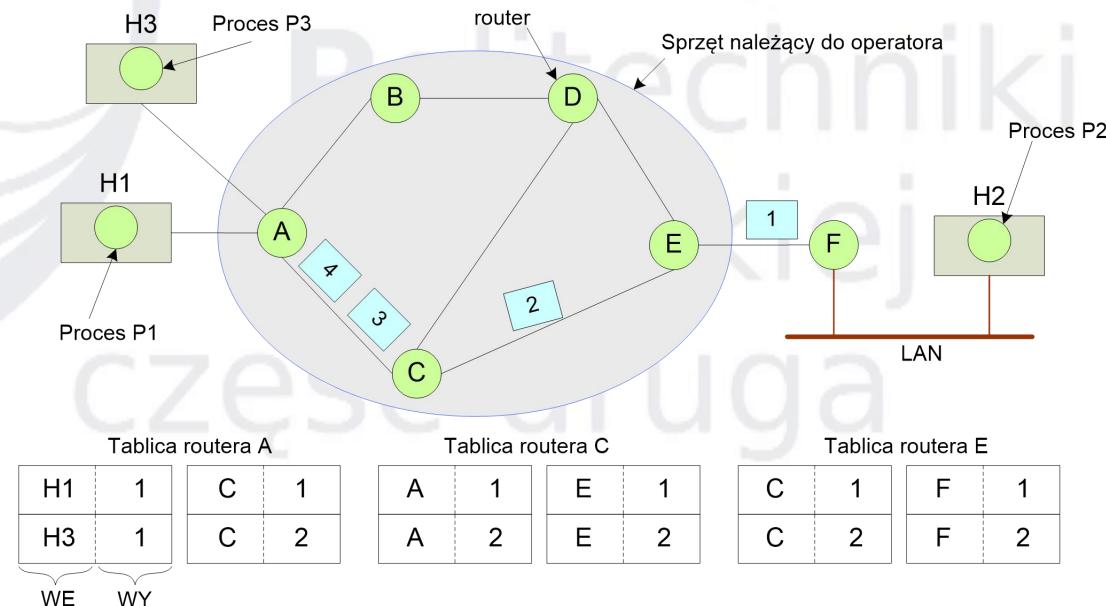
- Rola warstwy sieciowej w sieciach
- Dostarczenie pakietów (datagramów) od źródła do celu (rutowanie)
- Pakiet (datagram) posiada wszystkie informacje, pozwalające na routing i rozpoznawanie przez odbiorców (analogia listu poleconego)
- Router może zwrócić informację o braku możliwości dostarczenia pakietu za pomocą ICMP
- Usługa połączeniowa a usługa bezpołączeniowa

# Implementacja u. połączeniowej

- Rola warstwy sieciowej w sieciach
- połączenie tworzy tzw. **obwód wirtualny VC (virtual circuit)**
- podsieć = **podsieć obwodów wirtualnych**
- VC => unikanie wyboru nowej trasy dla każdego wysyłanego pakietu

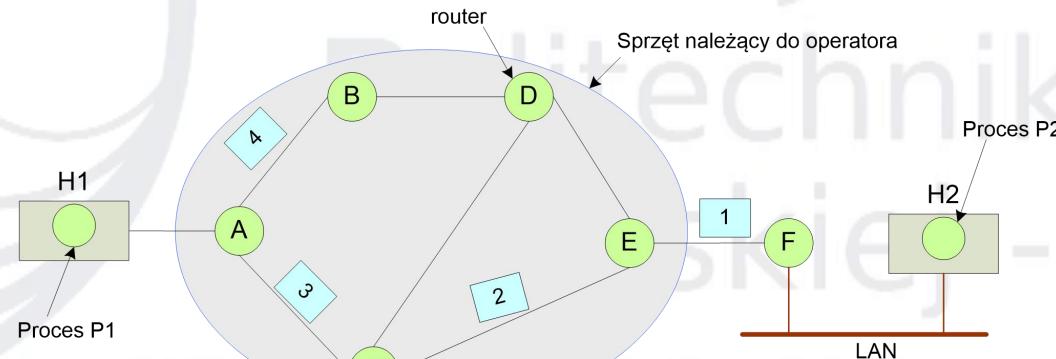
## ETYKIETOWANIE:

Router A odróżnia pakiety połączenia nr1 z H1 od pakietów z połączenia nr2 z H2, to C tego nie potrafi, dlatego A przydziela **inny identyfikator połączenia ruchowi wychodzącemu dla drugiego połączenia**



# Implementacja u. połączeniowej

- Pakiety są wprowadzane do sieci indywidualnie i niezależnie
- Pakiety = datagramy, podsieć = **podsieć datagramowa**
- Algorytm zarządzający tablicami i podejmujący decyzje o wyborze trasy nazywa się **algorytmem routingu**



Tablica routera A początkowo		po później	
A	-	A	-
B	B	B	B
C	C	C	C
D	B	D	B
E	C	E	B
F	C	F	B

Tablica routera C	
A	A
B	A
C	-
D	D
E	E
F	E

Tablica routera E	
A	C
B	D
C	C
D	D
E	-
F	F

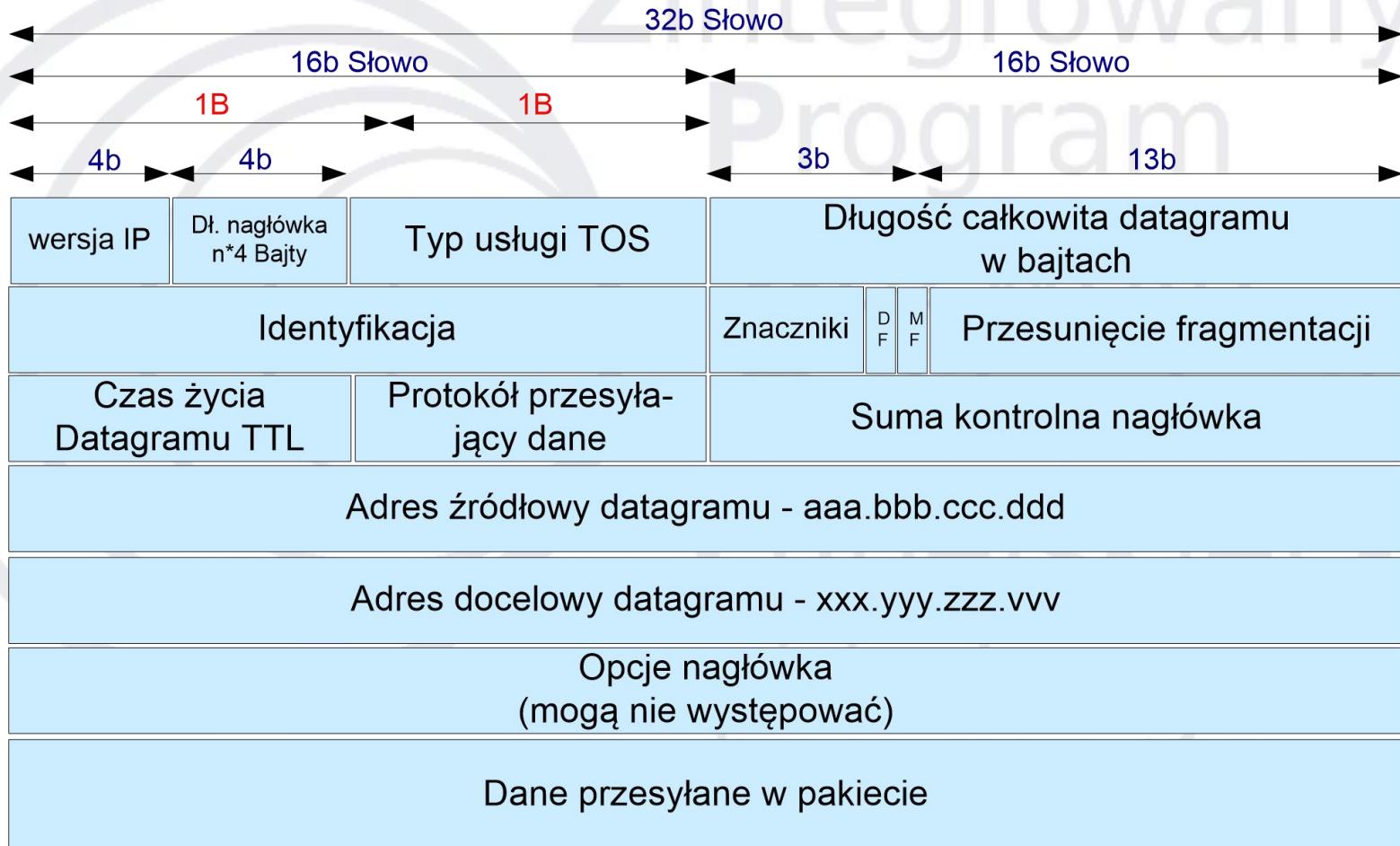
# Obwody datagramowe vs. wirtualne

Problem	Podsieć datagramowa	Podsieć obw. wirtualnych
Zestawianie obwodu	Niepotrzebne	Wymagane
Adresowanie	Każdy pakiet zawiera pełny adres źródłowy i docelowy	Każdy pakiet zawiera numer VC
Informacje o stanie	Brak zapamiętywania przez routery danych stanu połączeń	Każdy VC wymaga na każde połączenie miejsca w tablicy routera
Routing	Każdy pakiet jest kierowany niezależnie	Trasa wybierana przy zestawianiu VC, podążają nią wszystkie pakiety
Skutki problemów z routerem	Żadne poza pakietami utraconymi w chwili awarii	Wszystkie VC przechodzące przez router w trakcie awarii zostają zerwane
Zapewnienie QoS	Trudne	Łatwe: do każdego VC można przydzielić wystarczające zasoby

# Protokół IP – cechy podstawowe

- **Internet Protocol** jest przykładem sieci protokołu bezpołączeniowego co oznacza, że jest w stanie obsługiwać wymianę danych pomiędzy dwoma hostami z pominięciem fazy uprzedniego nawiązywania połączenia
- IP nie zapewnia **korekcji błędów**, nie jest też w stanie zapewnić w skrajnym przypadku, że część pakietów może zginieć
- IP **ukrywa strukturę sieci przed użytkownikiem** co oznacza, że z punktu widzenia użytkownika tworzy sieć wirtualną pomiędzy jego komputerem a komputerem, z którym wymieniane są dane; „**przezroczystość**” sieci uzyskuje się poprzez **enkapsulację**; pozwala to na łatwą instalację i konfigurację sieci opartych o IP
- IPv4 obsługuje **fragmentację** czyli potrafi dzielić poszczególne transmitowane PDU na mniejsze jednostki

# Datagram IPv4



# Protokół trasowania

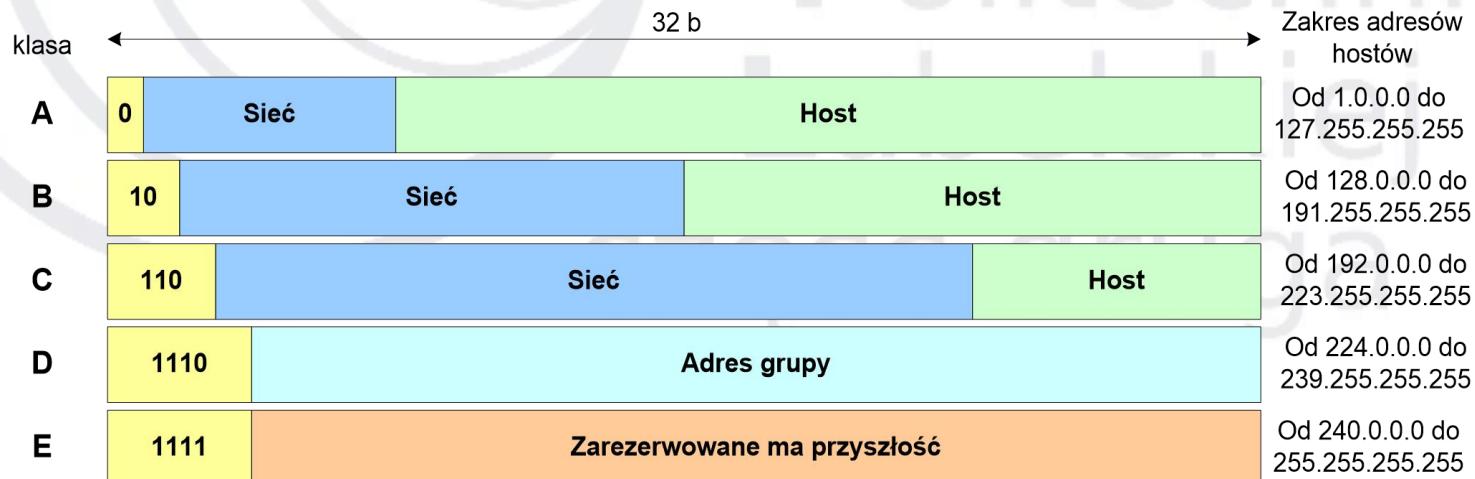
- **Protokół trasowania, protokół routingu, protokół routujący** – protokół używany do wymiany informacji o trasach pomiędzy sieciami komputerowymi, z zastosowaniem dynamicznej budowy tablic trasowania
- Tradycyjne trasowanie polega na wykorzystaniu tylko informacji o **następnym „przeskoku”** (ang. *hop*), przy czym router kieruje pakiet do następnego routera, bez uwzględnienia obciążenia czy awarii na dalszej części trasy
- **Trasowanie dynamiczne** wpłynęło na elastyczność i rozwój Internetu

# Protokół IP - hierarchia przestrzeni adresowej

- Hierarchia przestrzeni adresowej IP można określić mianem **złożonej** ze względu na dwa aspekty:
- W każdym adresie IP można wyróżnić dwa poziomy
- Klasy adresów definiowane są w oparciu o alokację bitów na obu poziomach. Podział łańcucha bitów na cztery ośmiobitowe fragmenty, w wyniku czego powstają grupy logiczne => tworzenie klas
- Każdy adres IP składa się z **adresu sieci i adresu hosta** umożliwiając wskazanie punktu końcowego
- Wpływają na wydajność operacyjną stacji roboczej
- (każdy z punktów końcowych musi mieć przydzielony unikatowy adres IP, ale wszystkie mogą korzystać z tego samego adresu sieci -> 'pamięć' ścieżki dostępu do danej sieci)
- Wszystkie hosty wewnątrz jednego adresu sieci należą do tego samego bloku adresowego

# Protokół IP – klasy adresów

- Podział przestrzeni na zakresy numeryczne
  - zarezerwowane dla małych średnich i dużych firm
  - każdy zakres pełni inne zadania
  - klasa zapewnia możliwość zdefiniowania innej liczby hostów
  - klasy oznaczono pojedynczymi literami alfabetu A, B, C, D, E
  - kompromis pomiędzy ilością adresowalnych sieci i hostów



# Wady adresowania klasowego

- "prosta elegancja", ale nie uwzględnia rozwoju i demografii Internetu
- Zaspokoiliła potrzeby sieci przez dekadę (do 1990r.)
- Ogromne różnice pojemności poszczególnych klas, które powodują zmniejszenie wydajności całego systemu i są przyczyną marnotrawienia jego fragmentów
- „pięta achillesowa” IPv4

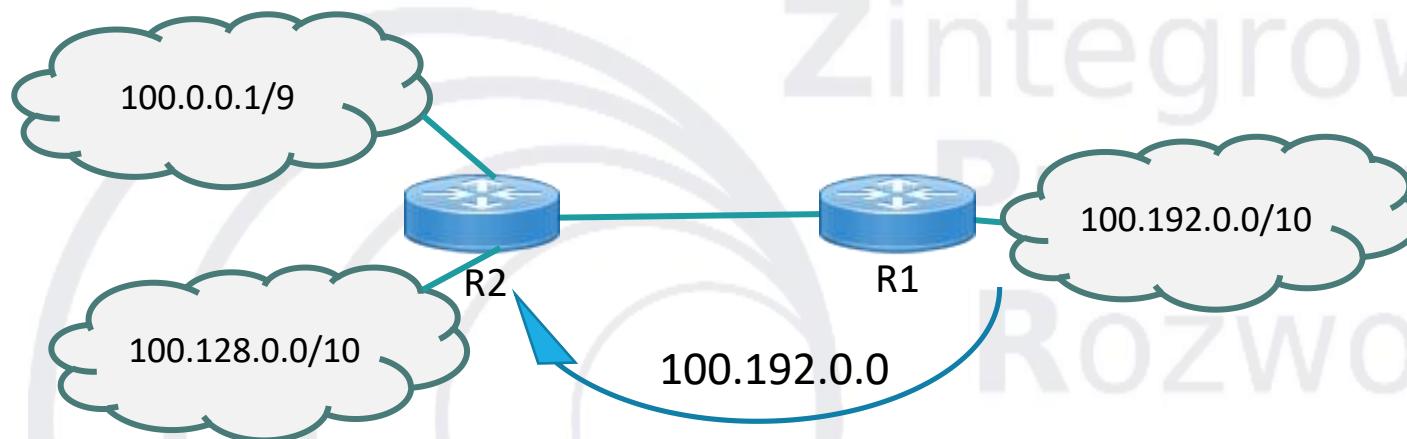
# FLSM – Maski o stałej długości

- **Fixed-Length Subnet Mask, FLSM**
  - Stanowi uzupełnienie dwuwarstwowej hierarchii (32b adresy składające się z części: sieci i hosta) o obsługę trzeciej warstwy
  - Pozwala tworzyć i adresować mniejsze sieci na bazie identyfikatorów większych sieci i sieciowych przestrzeni adresowych
  - Adres podsieciowy służy do adresowania danych w podsieciach
  - Przyczyny wprowadzenia:
    - korzystanie z Internetu za pośrednictwem pojedynczych ? => sieć LAN
    - Era architektury klient/serwer
    - podział sieci na segmenty dla celów poprawy wydajności
    - Wymuszenie podziału na segmenty poprzez odległość między węzłami LAN

# VLSM-Maski o zmiennej długości

- Przykład VLSM
- Wszystkie podsieci:
  - 150.10.0.0 /18
  - 150.10.128.0 /18
  - 150.10.192.0 /18
  - 150.10.64.0 /20
  - 150.10.80.0 /20
  - 150.10.96.0 /20
  - 150.10.112.0 /20
- rutery znajdujące się poza siecią 150.10.0.0 /16 mogą utrzymywać tylko jeden wiersz w swoich tablicach tras, zawierający wyłącznie sieć 150.10.0.0 /16
- trasy do podsieci muszą być zapamiętane w ruterach wewnętrz sieci 150.10.0.0 /16

# Warunek stosowalności VLSM



Protokoły wspierające VLSM:

- RIP v2 (IETF)
- OSPF (IETF)
- EIGRP (Cisco)

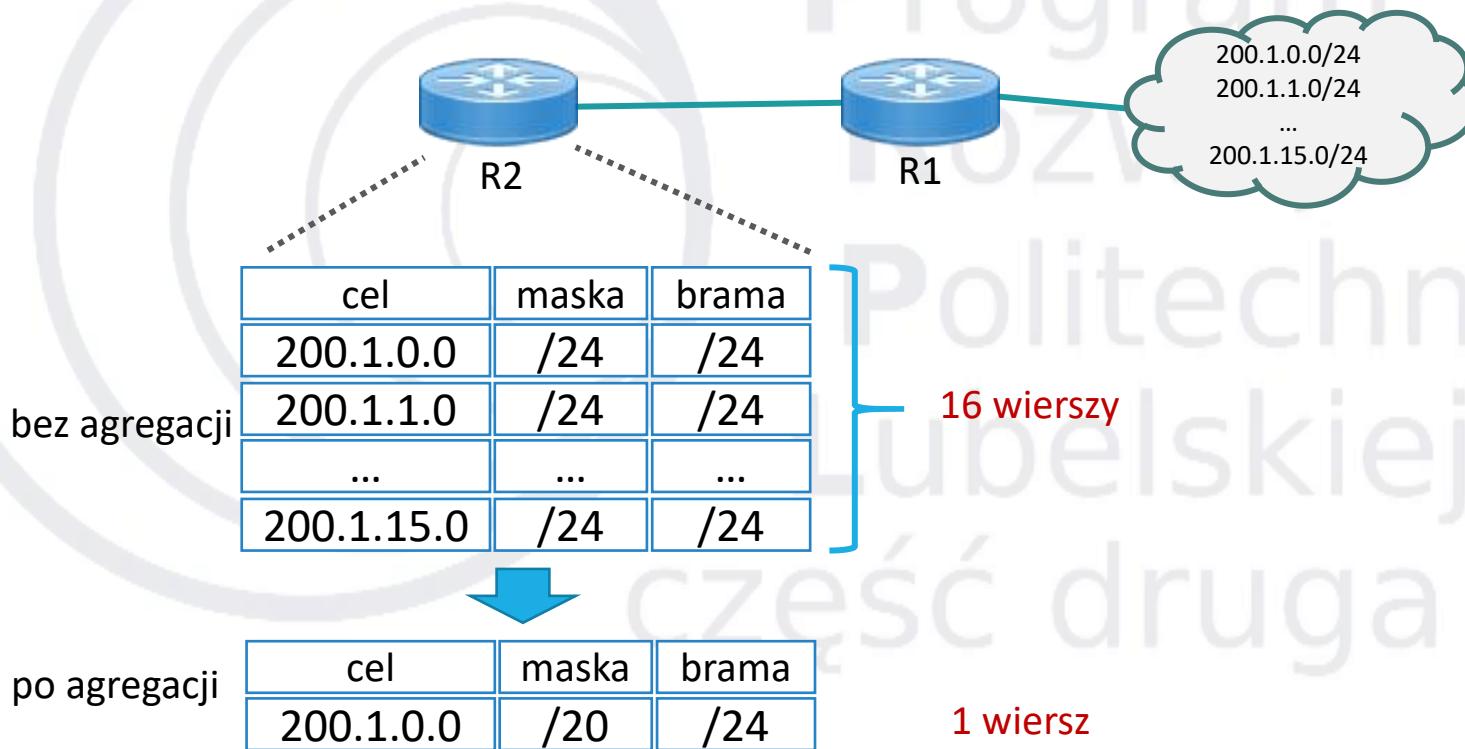
- Przykład VLSM
- Założmy, że routery R1 i R2 ustalają trasy protokołem dynamicznego wyboru tras (np. RIP)
- zastosowano VLSM dla sieci 100.0.0.0 /8
- Problem:
  - ruter R2 wysyła do R1 informację o sieci 100.192.0.0; jaką maskę ma przyjąć R1 dla tej sieci?
  - rozwiązanie (warunek stosowalności) –w komunikatach protokołu należy obok informacji o sieci przesyłać również maskę

# CIDR

- **CIDR** (RFC 1519) – *Classless InterDomain Routing* – oparty o przydzielanie pozostałych adresów IP w blokach o różnych wielkościach, bez zwracania uwagi na klasy
  - każdy wpis w tablicy routingu jest rozszerzany o 32b maskę => jedna tablica routingu dla wszystkich sieci, składająca się z macierzy trójek (adres IP, maska podsieci, linia wyjściowa)
  - porzucenie podejścia klasowego
  - pozwala zmniejszyć rozmiary tablic tras w ruterach-**agregacja adresów** sieci
  - narzuca przydział adresów, odpowiadający potrzebom-pojęcie „**sieci danej klasy**” zastąpione pojęciem „**blok adresów CIDR**”, w którym istotna jest tylko długość maski
  - technologia, zgodnie z którą dostawcy usług internetowych przydzielają adresy IP, stosowana razem z VLSM

# CIDR - agregacja adresów sieci

- Agregacja adresów => zmniejszenie rozmiaru tablic tras



# Odwzorowanie adresów

- Odwzorowanie adresów IP na adresy MAC (np. Ethernet) jest niezbędne dla realizacji operacji nadawczych, a dokładniej do konstrukcji prawidłowej ramki MAC
- Zadaniem tym zajmuje się protokół **ARP (Address Resolution Protocol)**, w oparciu o transmisję rozgłoszeniową zapytań
- Zbiera odpowiedzi bez zapewnienia poufności i autentyczności.
- Ze względu na efektywność, ARP wykorzystuje pamięć podręczną do składowania informacji pozyskanych z docierających zapytań i odpowiedzi ARP

Rodz. Adresu MAC	Rodz. Prot. sieciowego
Dl. Adr.	Dl. Adr.
MAC	Operacja ( zapytanie = 1 )
Siec.	Adres MAC Nadawcy
	Adres sieciowy Nadawcy
	Adres MAC Odbiorcy (=0)
	Adres sieciowy Odbiorcy

# Odwzorowanie adresów - RARP

- **RARP (Reverse Address Resolution Protocol)**
  - Dawniej, komputery bez dysku twardego pobierały adres IP z maszyny uprawnionej do świadczenia usług RARP, po przesłaniu zapytania z własnym adresem fizycznym
  - Host A rozwija zapytanie o swój adres IP do wszystkich hostów wraz ze swoim adresem fizycznym, wskazując siebie jako odbiorcę
  - Zapytanie dociera do wszystkich hostów w sieci, ale przetwarzają je i udzielają odpowiedzi tylko maszyny uprawnione do świadczenia usług RARP





Materiały zostały opracowane w ramach projektu  
„Zintegrowany Program Rozwoju Politechniki Lubelskiej – część druga”,  
umowa nr **POWR.03.05.00-00-Z060/18-00**  
w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020  
współfinansowanego ze środków Europejskiego Funduszu Społecznego

