

Sieci urządzeń mobilnych

Część 3 wykładu

SKO2

Mapa wykładu

- ❑ Wprowadzenie
 - Dlaczego mobilność?
 - Rynek dla mobilnych urządzeń
 - Dziedziny badań
- ❑ Transmisja radiowa
- ❑ Protokoły wielodostępowe
- ❑ Systemy GSM
- ❑ Systemy satelitarne
- ❑ Bezprzewodowe sieci lokalne

Historia komunikacji satelitarnej

- 1945 Arthur C. Clarke publikuje eseje o „Pozaziemskich przekaźnikach”
- 1957 pierwszy satelita: SPUTNIK!
- 1960 pierwszy satelita komunikacyjny ECHO
- 1963 pierwszy satelita geostacjonarny SYNCOM
- 1965 pierwszy komercyjny satelita geostacjonarny „Early Bird” (INTELSAT I): 240 dwukierunkowe kanały telefoniczne lub 1 kanał TV, okres życia 1.5 roku

Historia komunikacji satelitarnej

- 1976 trzy satelity MARISAT dla komunikacji morskiej
- 1982 pierwszy system satelitarnej telefonii mobilnej INMARSAT-A
- 1988 pierwszy system satelitarnej telefonii mobilnej z komunikacją danych INMARSAT-C
- 1993 pierwszy cyfrowy system telefonii satelitarnej
- 1998 globalne systemy satelitarne dla małych telefonów mobilnych

Zastosowania

□ Telekomunikacyjne

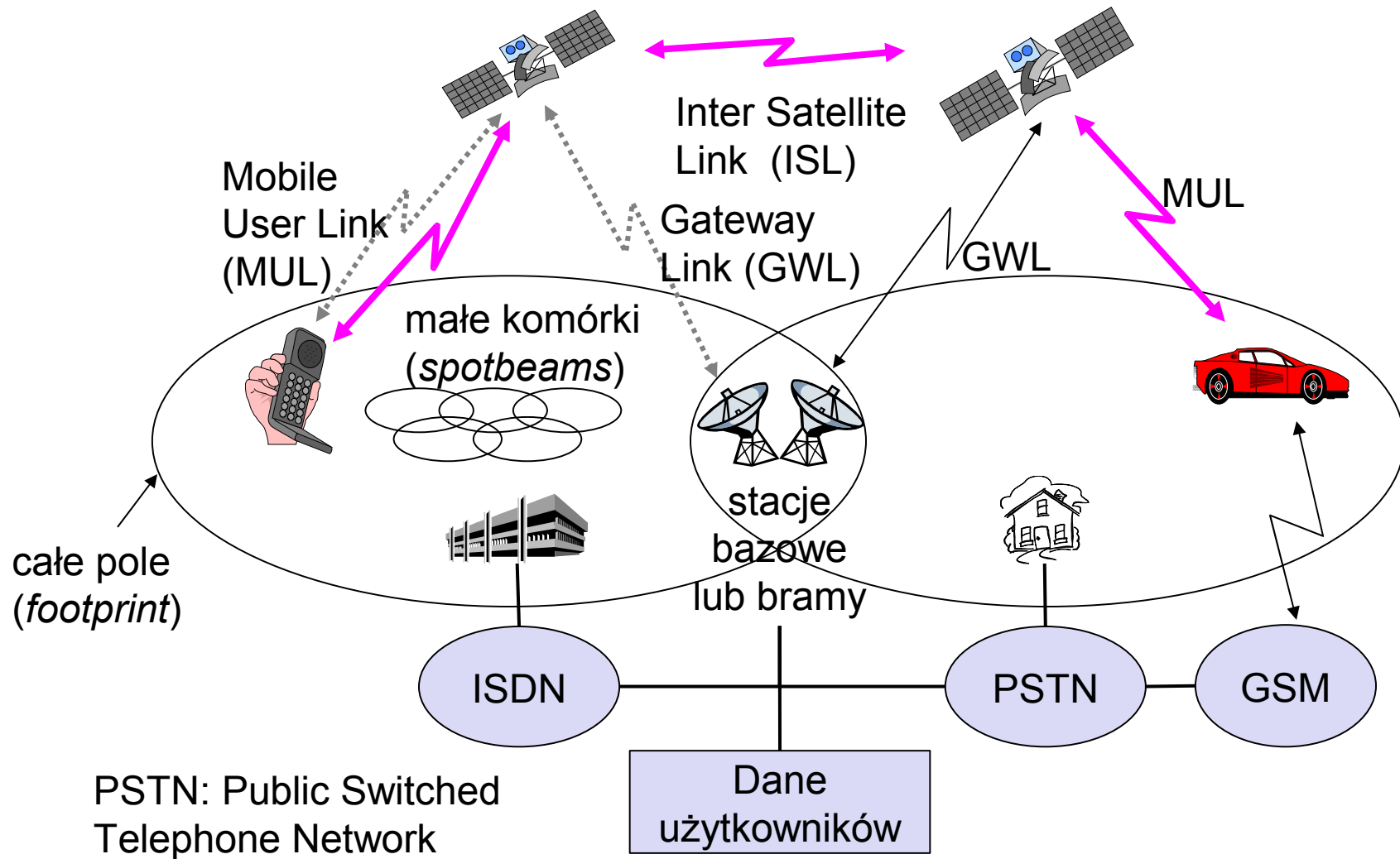
- globalne połączenia telefoniczne
 - szkielet dla sieci globalnych
 - komunikacja w odległych lub słabo rozwiniętych obszarach geograficznych
 - globalna komunikacja mobilna
- } zastąpione przez sieci światłowodowe

□ Inne

- satelity pogodowe
- satelity rozsyłające radia i telewizji
- satelity militarne
- satelity dla nawigacji i lokalizacji (n.p., GPS)

- → systemy satelitarne mające na celu rozszerzenie systemów komórkowych (n.p., GSM lub AMPS)

Klasyczny system satelitarny



Podstawy

□ Satelity na orbitach kołowych

- siła przyciągania $F_g = m g (R/r)^2$

- siła odśrodkowa $F_c = m r \omega^2$

- m : masa satelity

- R : promień ziemi ($R = 6370$ km)

- r : odległość satelity od środka ziemi

- g : przyciąganie grawitacyjne ($g = 9.81$ m/s²)

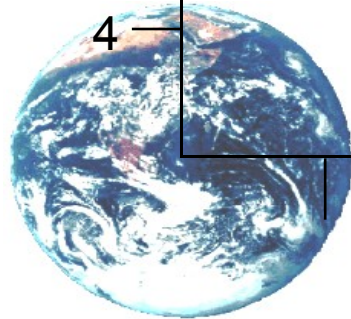
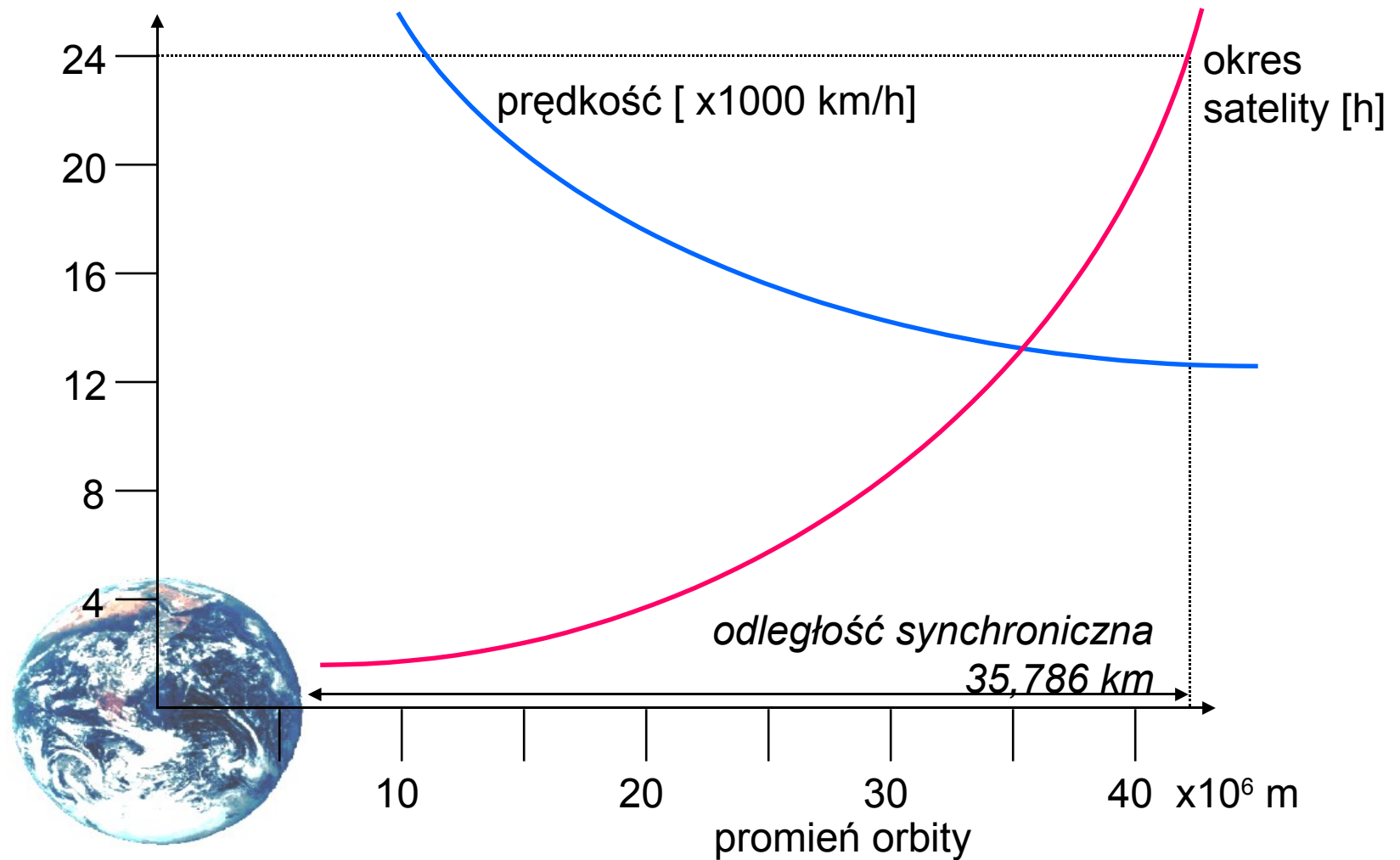
- ω : prędkość kątowa ($\omega = 2 \pi f$, f : częstotliwość obrotu)

$$r = \sqrt[3]{\frac{gR^2}{(2\pi f)^2}}$$

□ Stała orbita

- $F_g = F_c$

Okresy obrotu satelitów i orbity



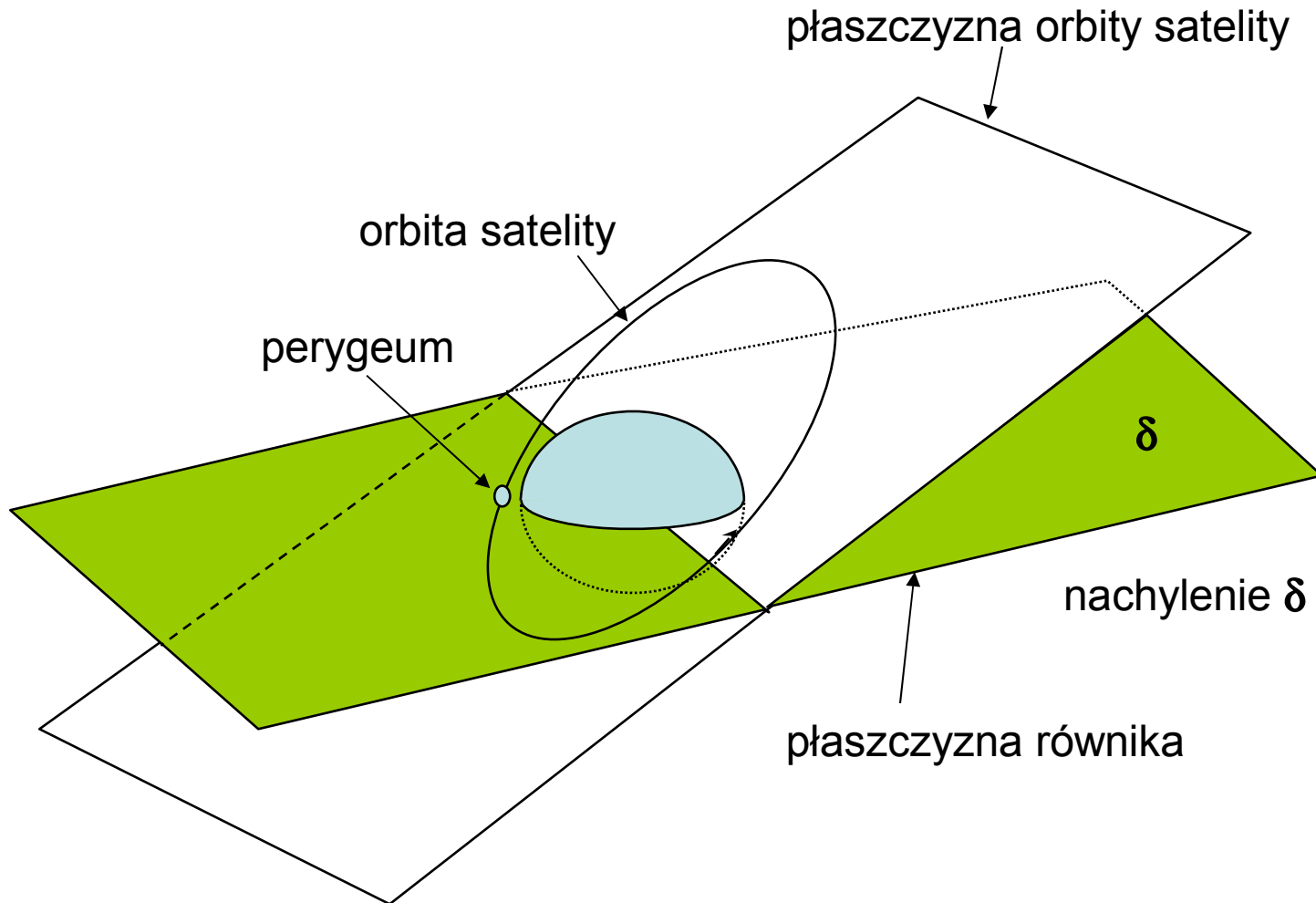
Podstawy

- ❑ orbity kołowe lub eliptyczne
- ❑ całkowity czas obrotu zależy od odległości satelity od Ziemi
- ❑ nachylenie: kąt pomiędzy orbitą a równikiem
- ❑ elewacja: kąt pomiędzy satelitą a horyzontem
- ❑ LOS (Line of Sight) do satelity konieczna dla połączenia
 - ➔ potrzebna wysoka elewacja, mniejsze zakłócenia przez n.p. budynki

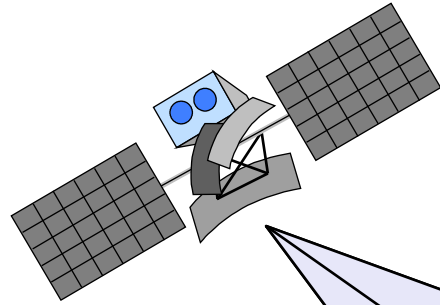
Podstawy

- ❑ Uplink: łącze od stacji bazowej do satelity
- ❑ Downlink: łącze od satelity do stacji bazowej
- ❑ zwykle, oddzielne częstotliwości na uplink i downlink
 - przełącznik na satelicie nadaje/odbiera i zmienia częstotliwości
 - przezroczysty przełącznik: tylko zmienia częstotliwości
 - regenerujący przełącznik: dodatkowo regeneracja sygnału

Nachylenie (inklinacja)



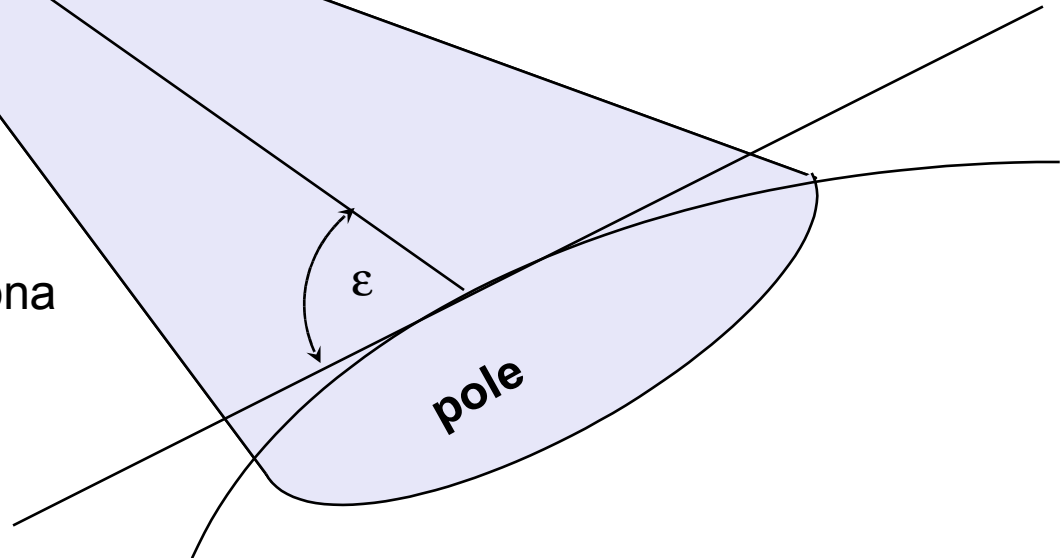
Elewacja



Elewacja:

kąt ε pomiędzy odcinkiem łączącym satelitę ze środkiem pola oraz płaszczyzną horyzontu (styczną do powierzchni ziemi)

minimalna elewacja:
najmniejsza elewacja potrzebna do komunikacji z satelitą



Łącza satelitarne

- Osłabienie i moc odbieranego sygnału określone są przez cztery parametry:

- moc nadawczą
- zysk anteny nadawczej
- odległość pomiędzy nadawcą a odbiorcą
- zysk anteny odbiorczej

L: strata

f: częstotliwość nośna

r: odległość

c: prędkość światła

$$L = \left(\frac{4\pi r f}{c} \right)^2$$

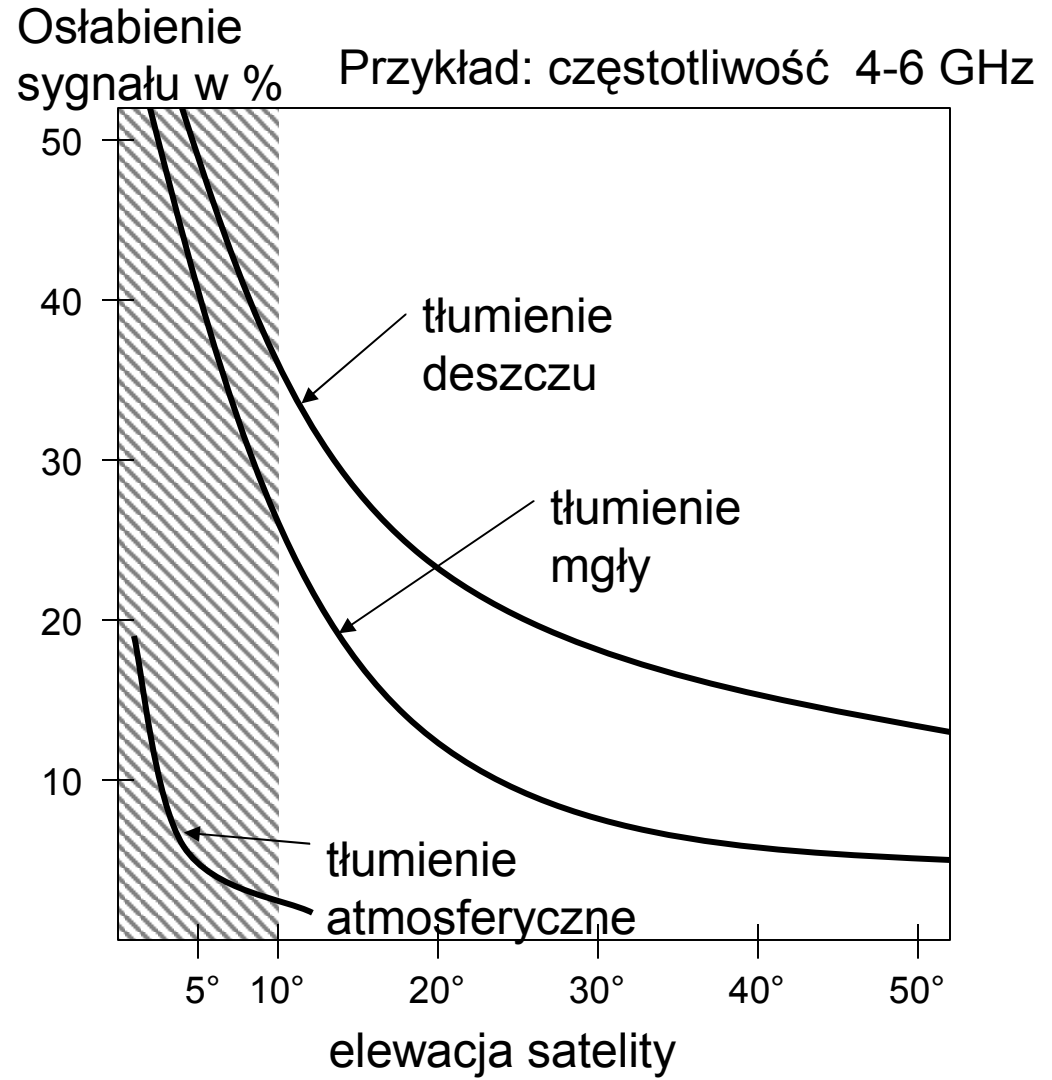
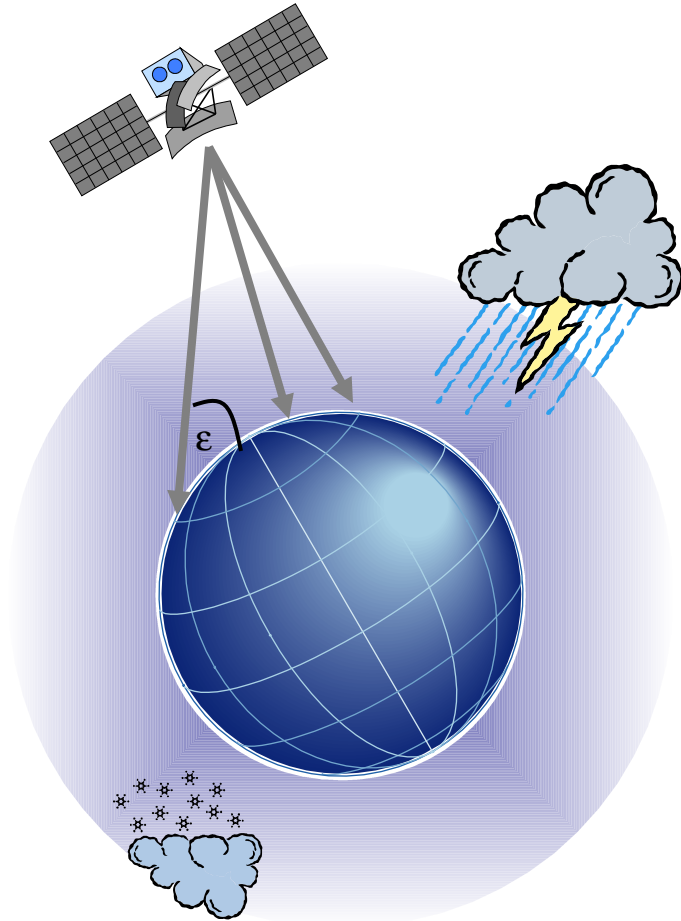
- Problemy

- zmienna moc odbieranego sygnału z powodu propagacji wielościeżkowej
- przerwania z powodu cienia (brak LOS)

- Możliwe rozwiązania

- Margines łącza eliminujący zmienność mocy sygnału
- różnorodność satelitów (użycie wielu widocznych satelitów jednocześnie) pozwala użyć mniejszej mocy nadawczej

Atmosferyczne tłumienie sygnału

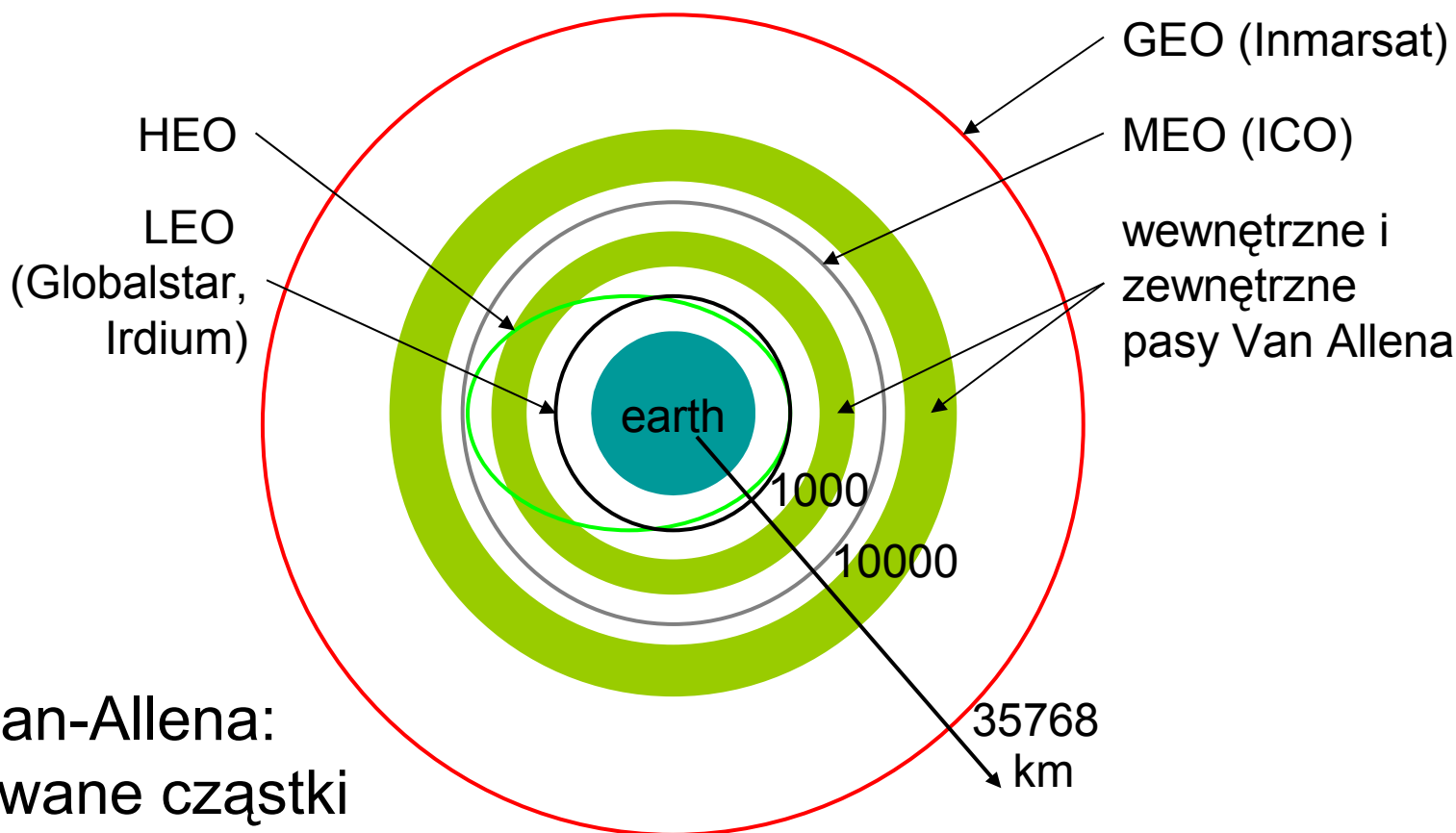




Orbity I

- Rozróżniamy cztery różne typy orbit satelitarnych w zależności od kształtu i średnicy orbity:
- GEO: orbita geostacjonarna, ok. 36000 km powyżej powierzchni ziemi
- LEO (*Low Earth Orbit*): ok. 500 - 1500 km
- MEO (*Medium Earth Orbit*) lub ICO (*Intermediate Circular Orbit*): ok. 6000 - 20000 km
- HEO (*Highly Elliptical Orbit*) orbity eliptyczne

Orbity II



Pasy Van-Allena:
zjonizowane cząstki
2000 - 6000 km i
15000 - 30000 km
nad powierzchnią ziemi

Satelity geostacjonarne



- Orbita 35,786 km od powierzchni ziemi, orbita w płaszczyźnie równika (nachylenie 0°)
 - → całkowity obrót dokładnie w jeden dzień, satelita jest zsynchronizowany z obrotem Ziemi
- pozycja anten może być stała, nie potrzeba jej zmieniać
- satelity zwykle mają duże pole (do 34% powierzchni Ziemi!), dlatego trudno jest ponownie używać częstotliwości

Satelity geostacjonarne



- ❑ złe elewacje w obszarach o szerokości geogr. powyżej 60° z powodu stałej pozycji nad równikiem
- ❑ potrzebna wysoka moc nadawcza
- ❑ duże opóźnienie ze względu na wysokość (ok. 275 ms)
 - → nie jest użyteczne dla globalnej komunikacji małych telefonów mobilnych i transmisji danych, typowo używany dla transmisji radiowej i telewizyjnej

Systemy LEO

- ❑ Orbita ok. 500 - 1500 km nad pow. Ziemi
- ❑ widoczność satelity przez ok. 10 - 40 minut
- ❑ możliwy globalny zasięg radiowy
- ❑ opóźnienie porównywalne z ziemską rozmową zagraniczną, ok. 5 - 10 ms
- ❑ mniejsze pola, lepsze wykorzystanie częstotliwości
- ❑ ale potrzebne przekazywanie od jednego satelity do drugiego
- ❑ potrzeba wiele satelitów dla globalnego zasięgu
- ❑ bardziej złożone systemy z powodu ruchomych satelitów



Systemy MEO

- ❑ Orbita ok. 5000 - 12000 km nad pow. Ziemi
- ❑ porównanie z systemami LEO:
 - mniejsza prędkość satelitów
 - potrzeba mniej satelitów
 - prostszy system
 - dla wielu połączeń, nie potrzeba przekazywania
 - większe opóźnienie, ok. 70 - 80 ms
 - potrzebna większa moc nadawcza
 - potrzebne specjalne anteny dla mniejszych pól

Ruting

- **Możliwe rozwiązanie: łączy pomiędzy satelitami**
 - potrzeba mniej bram
 - przekazywanie połączeń lub pakietów w obrębie sieci satelitarnej tak długo, jak to możliwe
 - tylko jeden uplink i downlink dla każdego końca połączenia potrzebny dla połączenia dwóch mobilnych telefonów
- **Problemy:**
 - bardziej złożone sterowanie antenami pomiędzy satelitami
 - duża złożoność systemu z powodu ruchomych ruterów
 - większe zużycie paliwa
 - dlatego krótszy okres życia satelity

Ruting połączeń w telefonii satelitarnej

- ❑ Mechanizm podobny do GSM
- ❑ Bramy utrzymują rejestry danych użytkownika
 - HLR (*Home Location Register*): statyczne dane
 - VLR (*Visitor Location Register*): (ostatnio znane) położenie stacji mobilnej
 - SUMR (*Satellite User Mapping Register*):
 - satelita przypisany do stacji mobilnej
 - położenie wszystkich satelitów
- ❑ Rejestracja stacji mobilnych
 - Lokalizacja stacji mobilnej przez pozycję satelity
 - żądanie danych użytkownika z HLR
 - aktualizacja VLR oraz SUMR
- ❑ Połączenie ze stacją mobilną
 - lokalizacja przez HLR/VLR podobnie jak w GSM
 - tworzenie połączenia przez odpowiedniego satelitę

Przekazywanie w systemach satelitarnych

- Ruch satelitów zwiększa częstość i złożoność przekazywania w porównaniu do systemów komórkowych
 - Przekazywanie w polu jednego satelity
 - handover z jednej komórki w polu do drugiej
 - stacja pozostaje w polu satelity, lecz zmienia komórkę
 - Przekazywanie pomiędzy satelitami
 - stacja mobilna opuszcza pole jednego, wchodzi w pole drugiego satelity
 - Przekazywanie pomiędzy bramami
 - stacja mobilna pozostaje w polu satelity, lecz zmienia bramę
 - Przekazywanie pomiędzy systemami
 - przekazywanie z sieci satelitarnej do ziemskiej sieci komórkowej

Mapa wykładu

- ❑ Wprowadzenie
 - Dlaczego mobilność?
 - Rynek dla mobilnych urządzeń
 - Dziedziny badań
- ❑ Transmisja radiowa
- ❑ Protokoły wielodostępowe
- ❑ Systemy GSM
- ❑ Systemy satelitarne
- ❑ Bezprzewodowe sieci lokalne

Cechy bezprzewodowych sieci LAN

□ Zalety

- bardzo elastyczne
- możliwe tworzenie sieci ad-hoc bez infrastruktury i planowania
- (prawie) nie ma problemów z przewodami
- bardziej odporne na sytuacje awaryjne i katastrofalne

□ Wady

- zwykle mała przepustowość w porównaniu do sieci przewodowych (1-10 Mb/s)
- wiele rozwiązań niestandardowych, szczególnie o wyższych przepustowościach, standardy powstają powoli (n.p. IEEE 802.11)
- produkty muszą być zgodne z regulacjami narodowymi dotyczącymi radia
 - stworzenie globalnych systemów trwa długo
- Bezpieczeństwo informacji

Cele projektowe sieci WLAN

- ❑ małe zużycie mocy
- ❑ technologia transmisyjna odporna na zakłócenia
- ❑ bezpieczeństwo informacji
- ❑ globalne działanie stacji mobilnych
- ❑ brak specjalnych licencji na używanie sieci WLAN
- ❑ prostota w użyciu
- ❑ ochrona inwestycji w sieci przewodowe
- ❑ bezpieczeństwo radiowe (niskie promieniowanie)
- ❑ przezroczystość dla warstwy aplikacji
- ❑ znajomość lokalizacji, gdy jest to potrzebne

Podczerwień a radio

❑ Podczerwień

❑ Zalety

- proste, tanie, dostępne w wielu urządzeniach mobilnych
- nie potrzeba licencji
- proste ekranowanie

❑ Wady

- interferencja ze światłem słonecznym, źródłami ciepła itd.
- łatwo zasłonić/wchłonąć światło IR
- mała przepustowość

❑ Przykład

- IrDA (*Infrared Data Association*)
 - interfejs dostępny wszędzie

❑ Radio

❑ Zalety

- można użyć doświadczenia z radiowych sieci WAN
- większy zasięg (radio przechodzi przez ściany, meble itd.)

❑ Wady

- bardzo niewiele częstotliwości bez licencji
- ekranowanie trudne, zakłócenia przez inne urządzenia elektryczne

❑ Przykład

- WaveLAN, HIPERLAN, Bluetooth

Bezprzewodowa sieć LAN IEEE 802.11

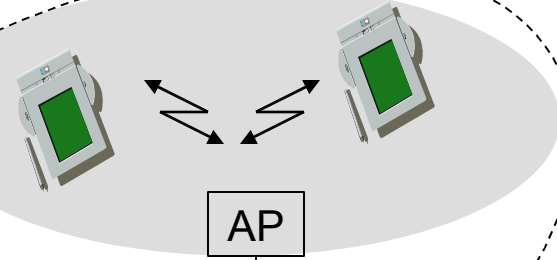


- **802.11b**
 - pasmo radiowe 2.4-5 GHz bez licencji
 - do 11 Mb/s
 - w warstwie fizycznej, używa *direct sequence spread spectrum* (DSSS)
 - wszystkie hosty używają tego samego kodu dzielącego
 - szeroko używane, korzysta z punktów dostępowych
- **802.11a**
 - pasmo 5-6 GHz
 - do 54 Mb/s
- **802.11g**
 - pasmo 2.4-5 GHz
 - do 54 Mb/s
- Używają CSMA/CA do wielodostępu
- Wszystkie mają wersję z punktami dostępowymi i ad-hoc

Sieci ad-hoc a infrastrukturalne

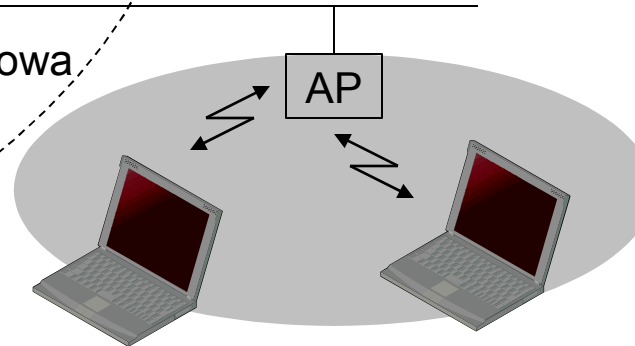
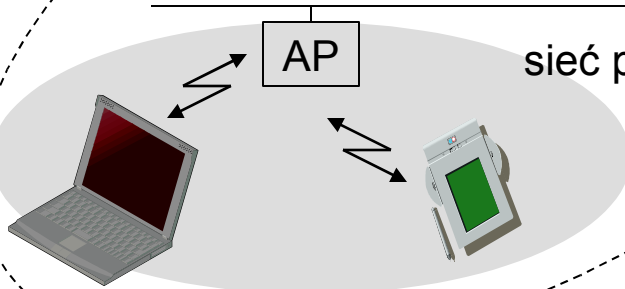


sieć
infrastrukturalna

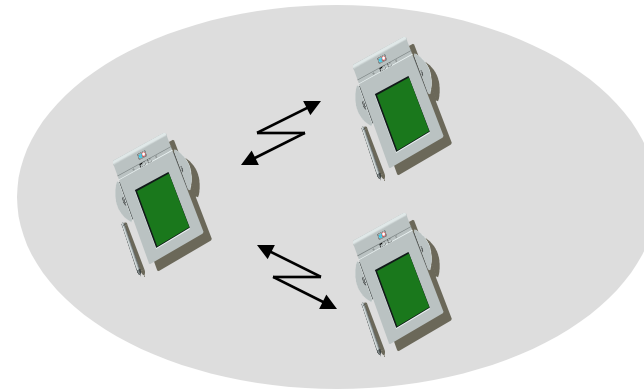
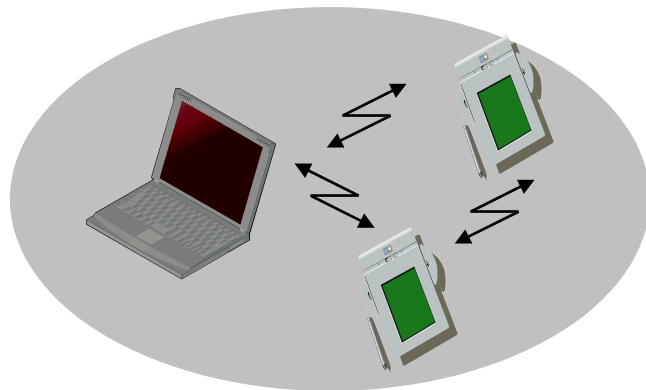


AP: Access Point

sieć przewodowa

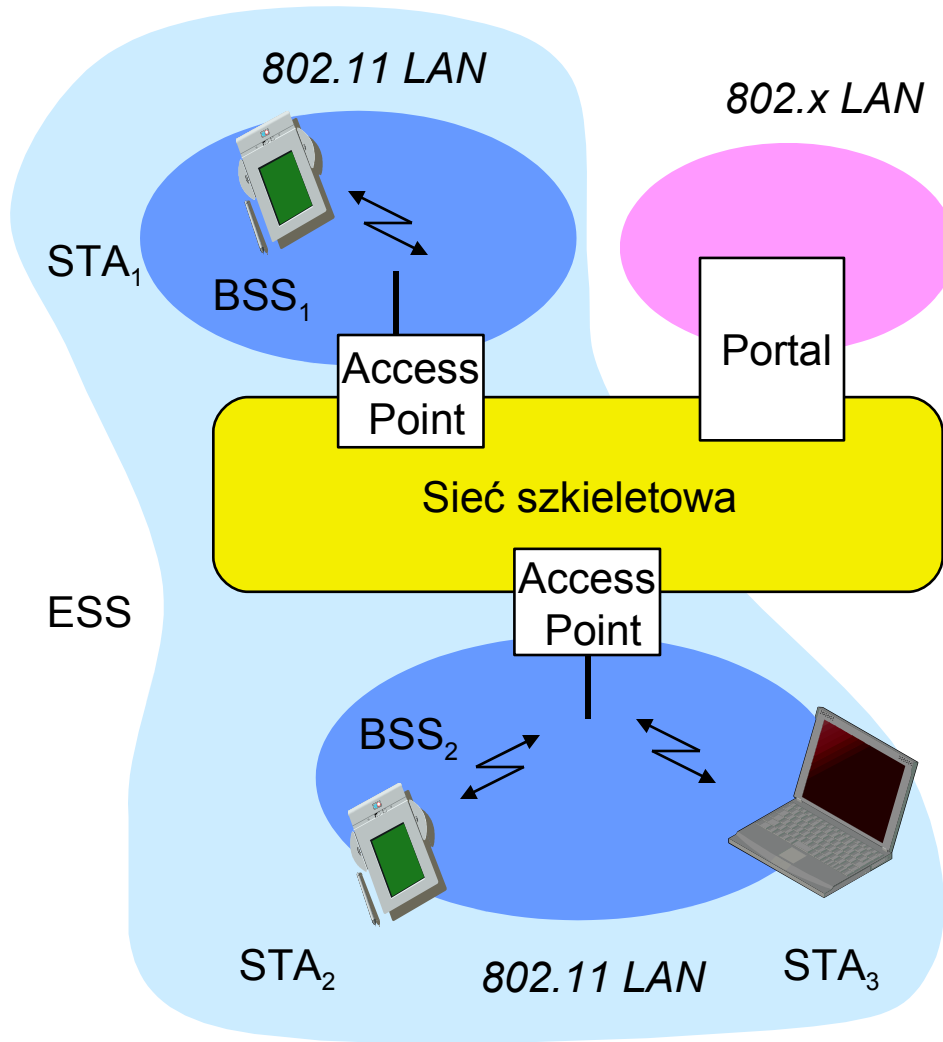


sieć ad-hoc



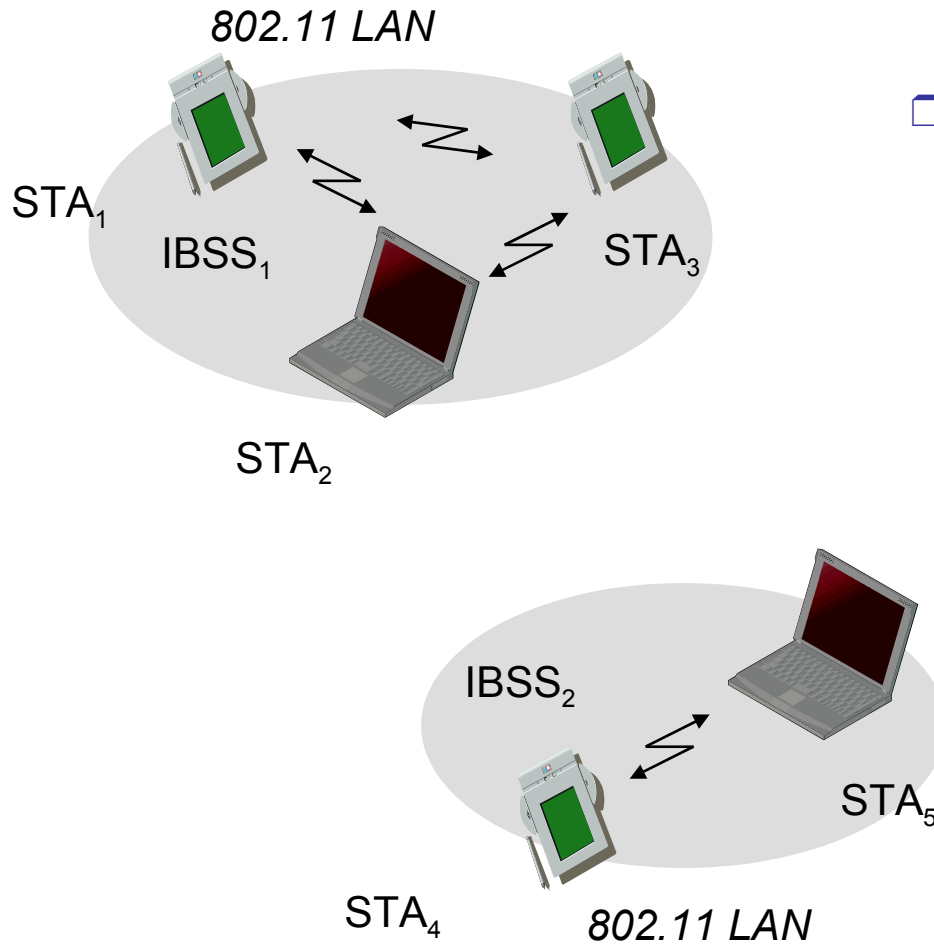


802.11 - architektura sieci infrastrukturalnej



- Stacja mobilna (STA)
 - terminal z łącznością radiową do punktu dostępowego
- *Basic Service Set* (BSS)
 - grupa stacji używających tej samej częstotliwości
- Punkt dostępowy
 - stacja połączona z siecią bezprzewodową i szkieletową
- Portal
 - most do innych sieci (przewodowych)
- Sieć szkieletowa
 - sieć łącząca sieci BSS w jedną logiczną sieć (EES: *Extended Service Set*)

802.11 - architektura sieci ad hoc

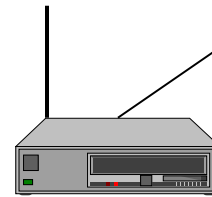
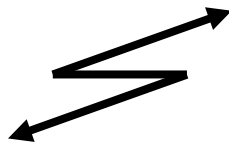


- Bezpośrednia komunikacja na mniejszym obszarze
 - Stacja (STA): terminal z dostępem do medium radiowego
 - *Independent Basic Service Set (IBSS)*: grupa stacji na tej samej częstotliwości

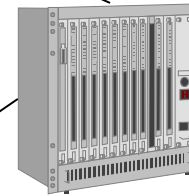


IEEE standard 802.11

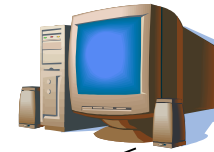
mobile terminal



access point



infrastructure network



fixed terminal

application
TCP
IP
LLC
802.11 MAC
802.11 PHY

LLC	
802.11 MAC	802.3 MAC
802.11 PHY	802.3 PHY

application
TCP
IP
LLC
802.3 MAC
802.3 PHY

802.11 - Warstwy i funkcje

□ MAC

- protokoły wielodostępowe, fragmentacja, szyfrowanie

□ Zarządzanie MAC

- synchronizacja, *roaming*, MIB, zarządzanie mocą

□ PLCP (*Physical Layer Convergence Protocol*)

- *carrier sense*

□ PMD (*Physical Medium Dependent*)

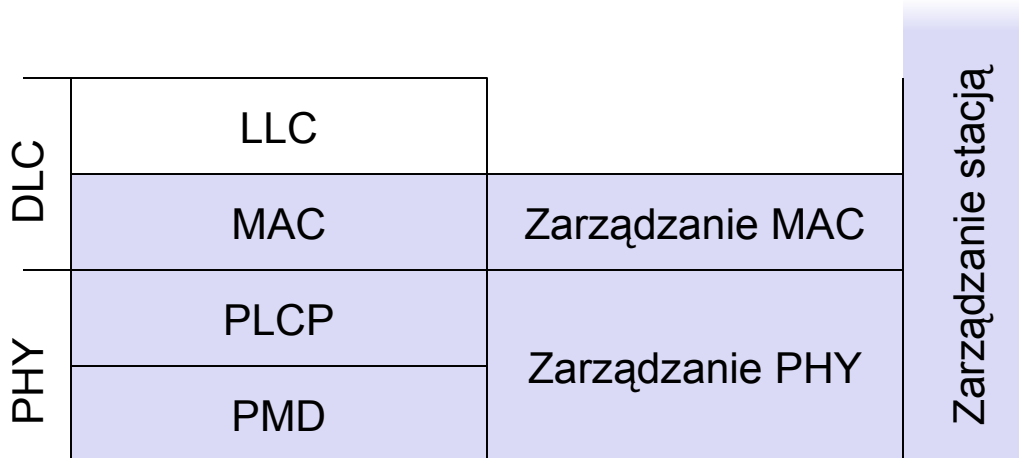
- modulacja, kodowanie

□ Zarządzanie PHY

- wybór kanału, MIB

Zarządzanie stacją

- koordynacja wszystkich funkcji zarządzania





802.11 - Warstwa fizyczna (podstawowa wersja)

- 3 wersje: 2 radiowe (zwykle 2.4 GHz), 1 w podczerwieni
 - przepustowości 1 do 2 Mb/s
 - FHSS (*Frequency Hopping Spread Spectrum*)
 - DSSS (*Direct Sequence Spread Spectrum*)
 - Podczerwień
- Warstwa fizyczna protokołu 802.11 została zastąpiona najpierw w wersji 802.11b, potem - w 802.11g

802.11 - warstwa MAC I - DFWMAC



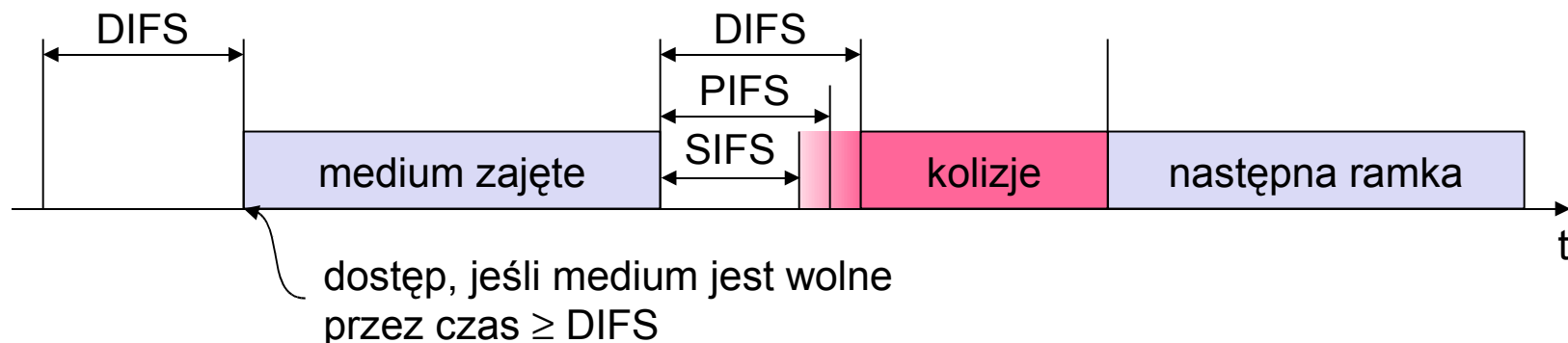
- Usługi ruchowe
 - Asynchroniczna usługa ruchowa (obowiązkowa)
 - wymiana pakietów przy jakości "best-effort"
 - możliwość komunikacji rozsiewczej
 - Usługa z gwarancją ograniczonego opóźnienia (opcjonalna)
- Metody dostępowe
 - DFWMAC-DCF CSMA/CA (obowiązkowe)
 - unikanie kolizji przez losowy mechanizm „cofania”
 - minimalna odległość w czasie pomiędzy pakietami
 - pakiet ACK dla potwierdzenia (nie przy broadcast)
 - DFWMAC-DCF z RTS/CTS (opcjonalne)
 - *Distributed Foundation Wireless MAC*
 - unika problemu z ukrytym terminalem
 - DFWMAC- PCF (opcjonalne)
 - punkt dostępowy odpytuje terminale według listy

802.11 - warstwa MAC II

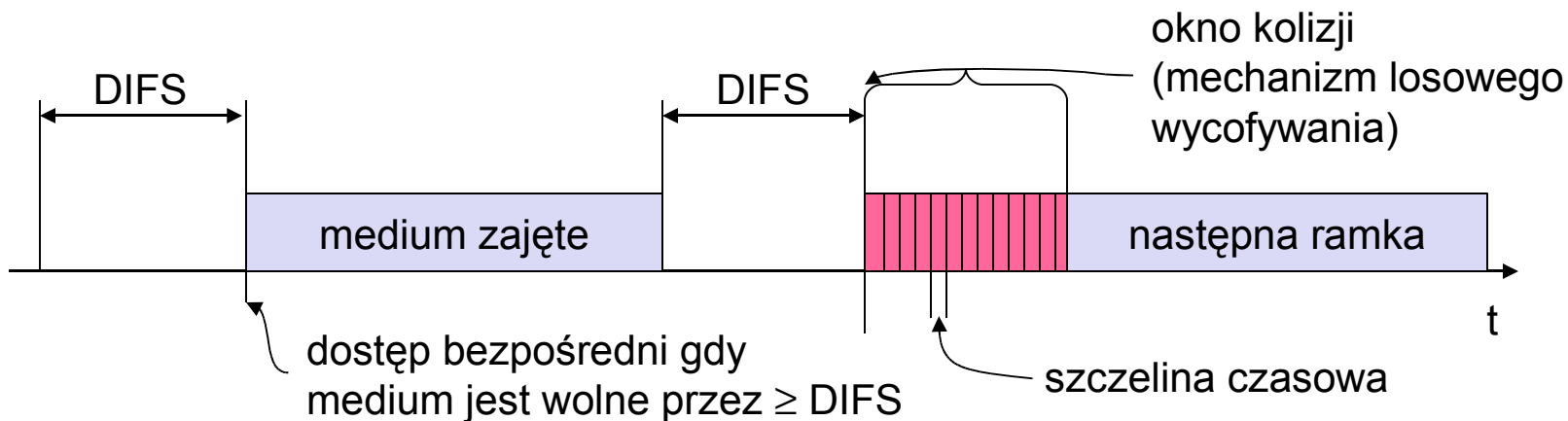


□ Priorytety

- określone przez różne odstępy między ramkami
- nie ma gwarantowanych, twardych priorytetów
- SIFS (*Short Inter Frame Spacing*)
 - najwyższy priorytet, dla ACK, CTS, odpowiedzi na odpytywanie
- PIFS (*PCF IFS*)
 - średni priorytet, dla usługi PCF (gwarancje maksymalnego opóźnienia)
- DIFS (*DCF, Distributed Coordination Function IFS*)
 - najniższy priorytet, dla usługi asynchronicznej

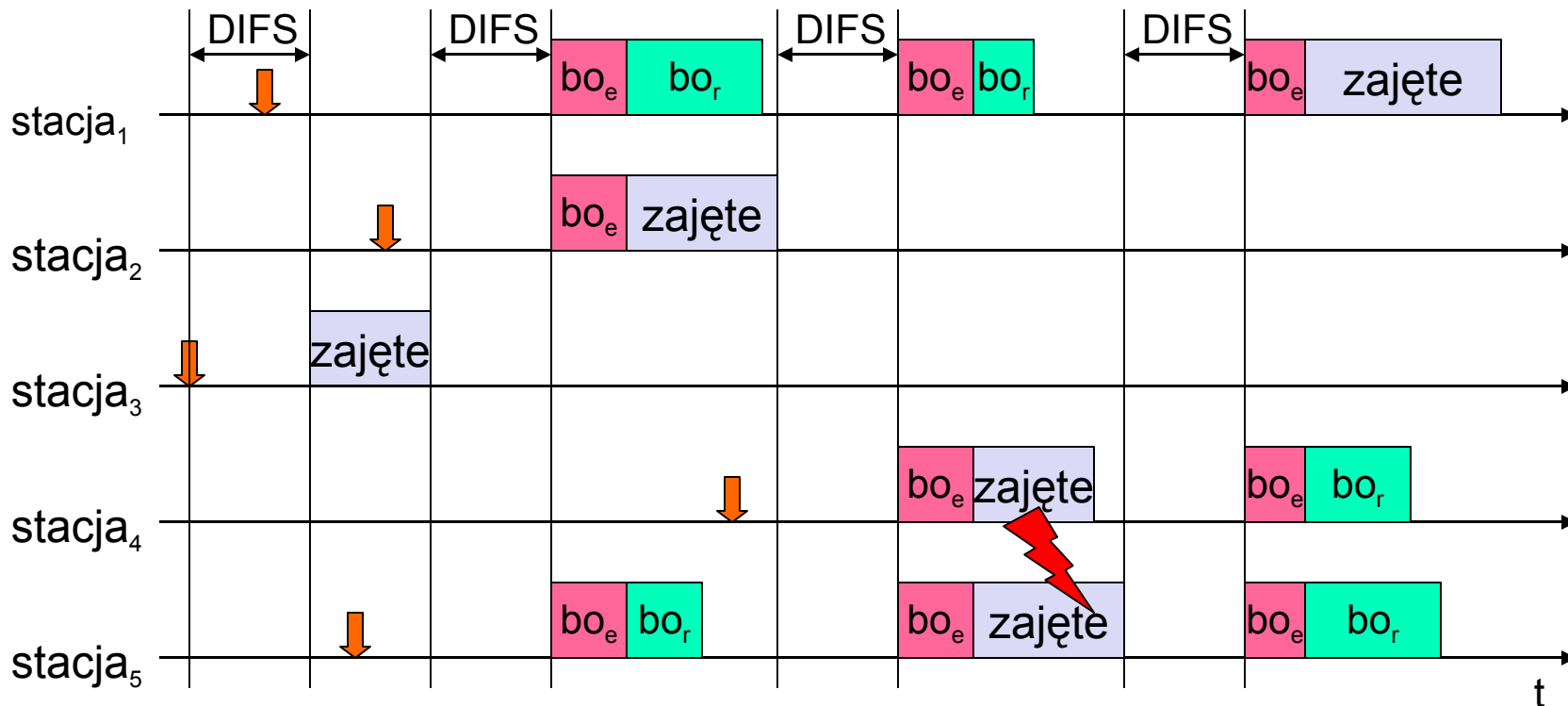


802.11 - protokół CSMA/CA



- stacja gotowa do nadawania rozpoczyna nasłuchiwanie medium (*Carrier Sense* w oparciu o *CCA, Clear Channel Assessment*)
- jeśli medium jest wolne przez okres *Inter-Frame Space* (IFS), stacja może rozpocząć nadawanie (IFS zależy od rodzaju usługi)
- jeśli medium jest zajęte, stacja musi czekać na wolny okres IFS, a potem dodatkowo czekać losowy czas wycofywania (unikanie kolizji, wielokrotność szczeliny czasowej)

802.11 - konkurujące urządzenia



zajęte

medium zajęte (ramka, ack itp.)

bo_e

czas wycyfowania



pakiet dochodzi do warstwy MAC

bo_r

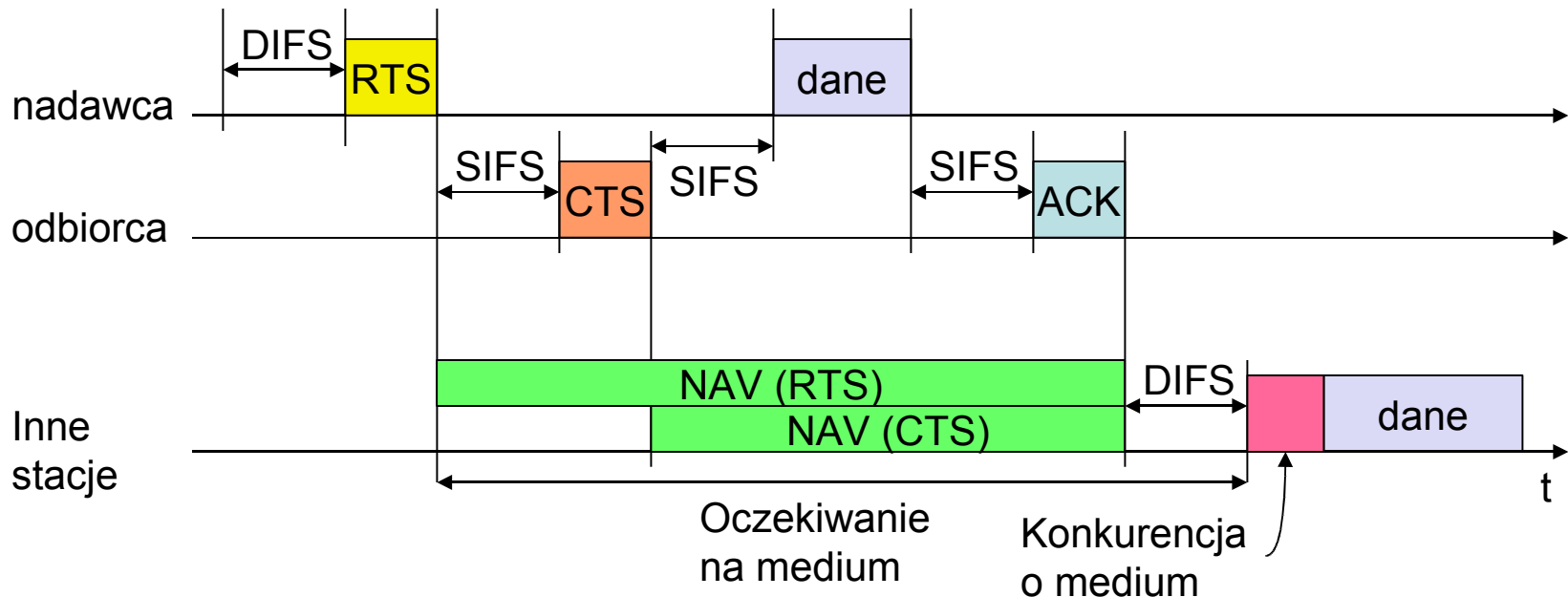
pozostały czas wycyfowania

802.11 - DFWMAC z RTS/CTS

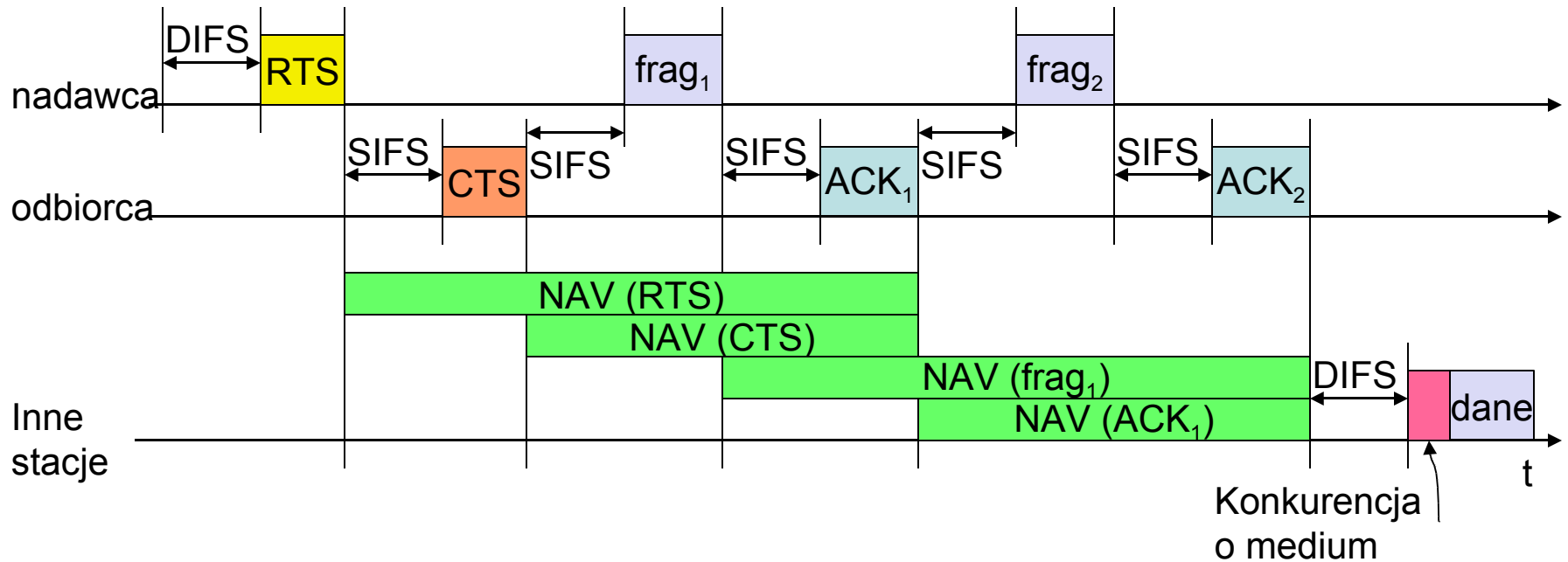


□ Wysyłanie pakietów unicast

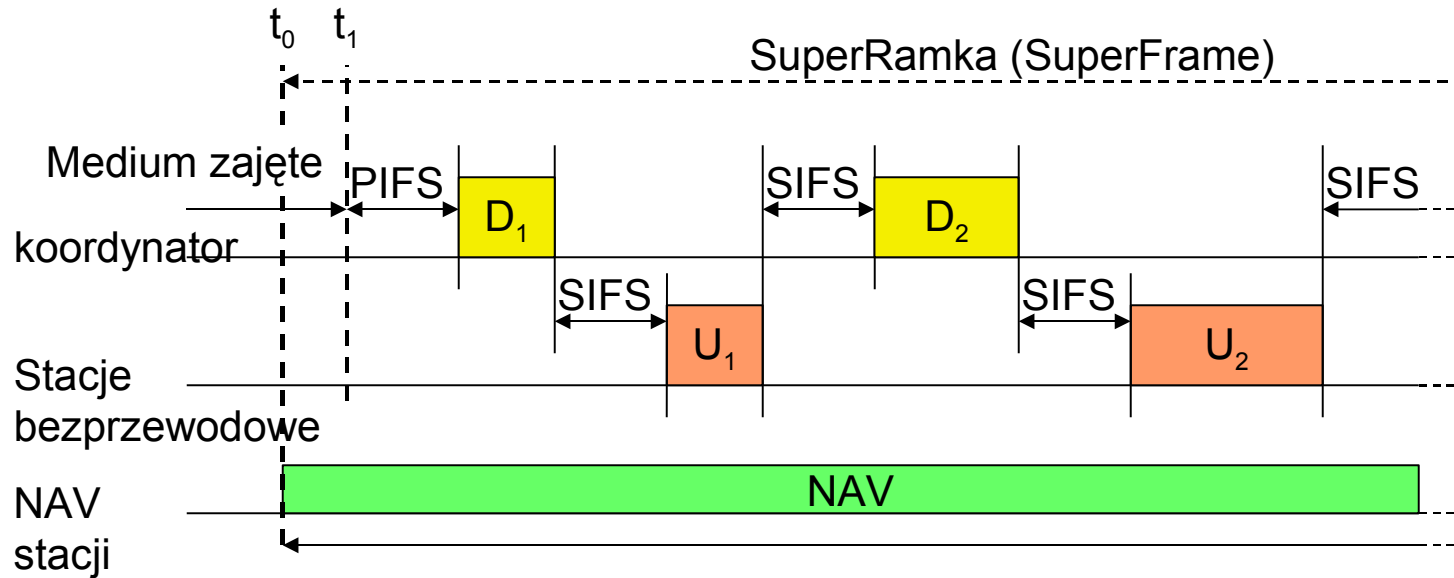
- Stacja może wysłać ramkę RTS z parametrami rezerwacji po odczekaniu czasu DIFS (rezerwacja określa, na jak długo potrzebne jest medium)
- Potwierdzenie przez ramkę CTS po czasie SIFS przez odbiorcę (jeśli jest gotów)
- Nadawca może wysłać dane od razu, potwierdzenie przez ramkę ACK
- Inne stacje zachowują rezerwacje otrzymane przez RTS i CTS w Net Allocation Vector (NAV)



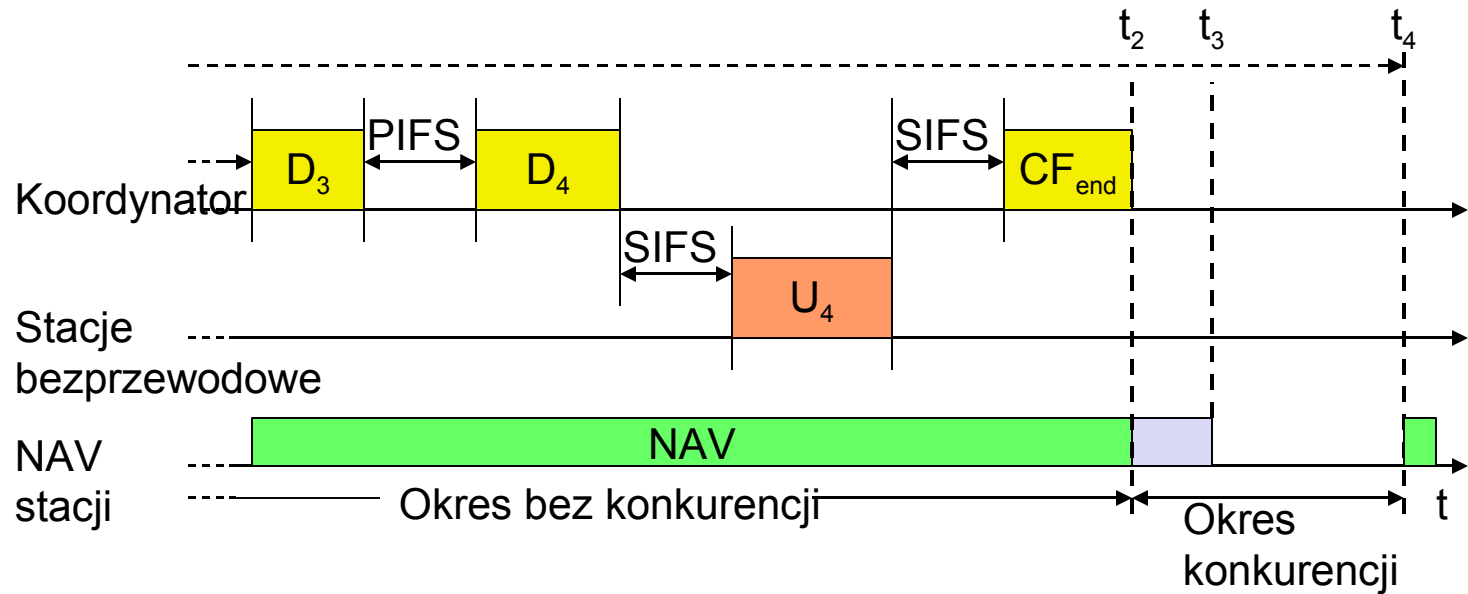
Fragmentacja



DFWMAC-PCF cz.I

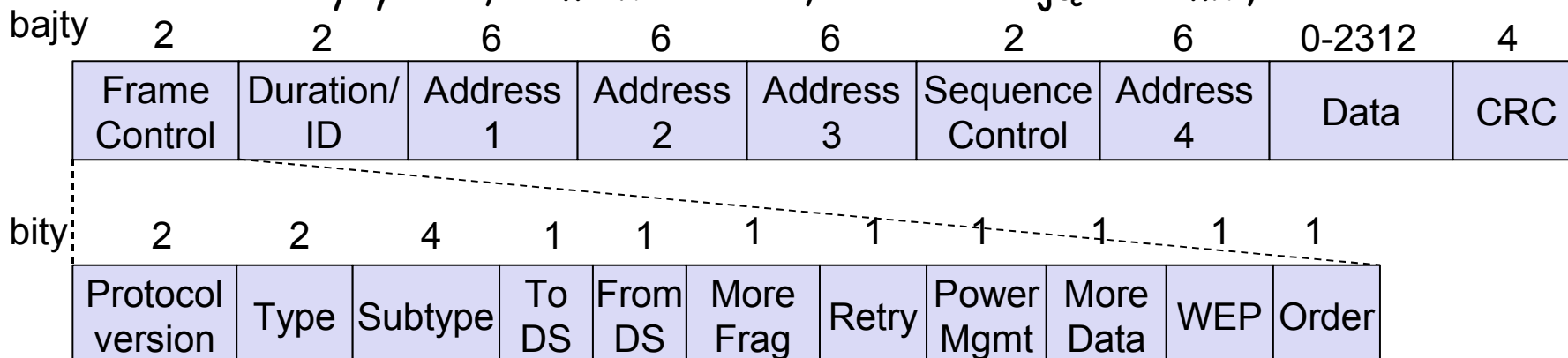


DFWMAC-PCF cz.II



802.11 - Format ramki

- Typy ramek
 - Ramki sterujące, ramki zarządzające, ramki danych
- Numery sekwencyjne
 - Potrzebne z powodu wielokrotnych transmisji po stracie ACK
- Adresy
 - nadawcy, odbiorcy (fizyczny), identyfikator BSS, nadawcy (logiczny)
- Różne
 - Czas wysyłania, suma kontrolna, dane sterujące ramki, dane



Znaczenie 4 adresów MAC

scenariusz	do DS	od DS	adres 1	adres 2	adres 3	adres 4
sieć ad-hoc	0	0	DA	SA	BSSID	-
sieć z infrastrukturą, od AP	0	1	DA	BSSID	SA	-
sieć z infrastrukturą, do AP	1	0	BSSID	SA	DA	-
sieć z infrastrukturą, w obrębie DS	1	1	RA	TA	DA	SA

DS: Distribution System

AP: Access Point

DA: Destination Address

SA: Source Address

BSSID: Basic Service Set Identifier

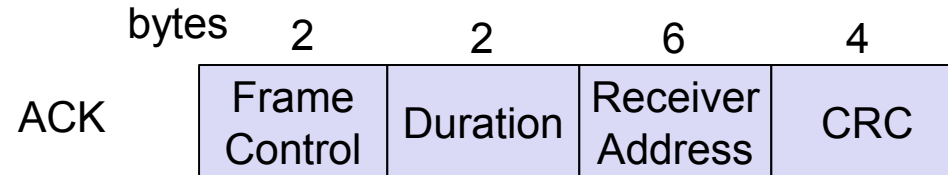
RA: Receiver Address

TA: Transmitter Address

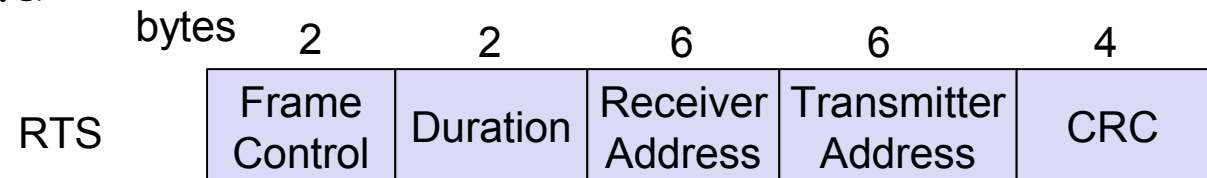
Ramki specjalne: ACK, RTS, CTS



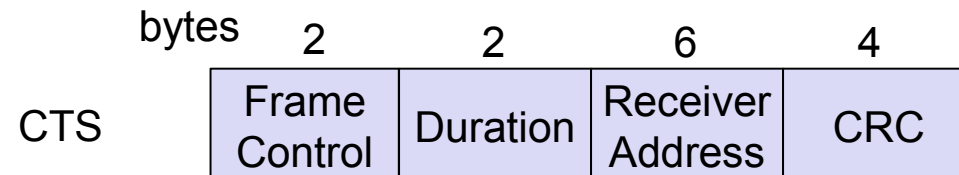
□ Potwierdzenie (ACK)



□ Request To Send



□ Clear To Send



802.11 - Zarządzanie w w. MAC

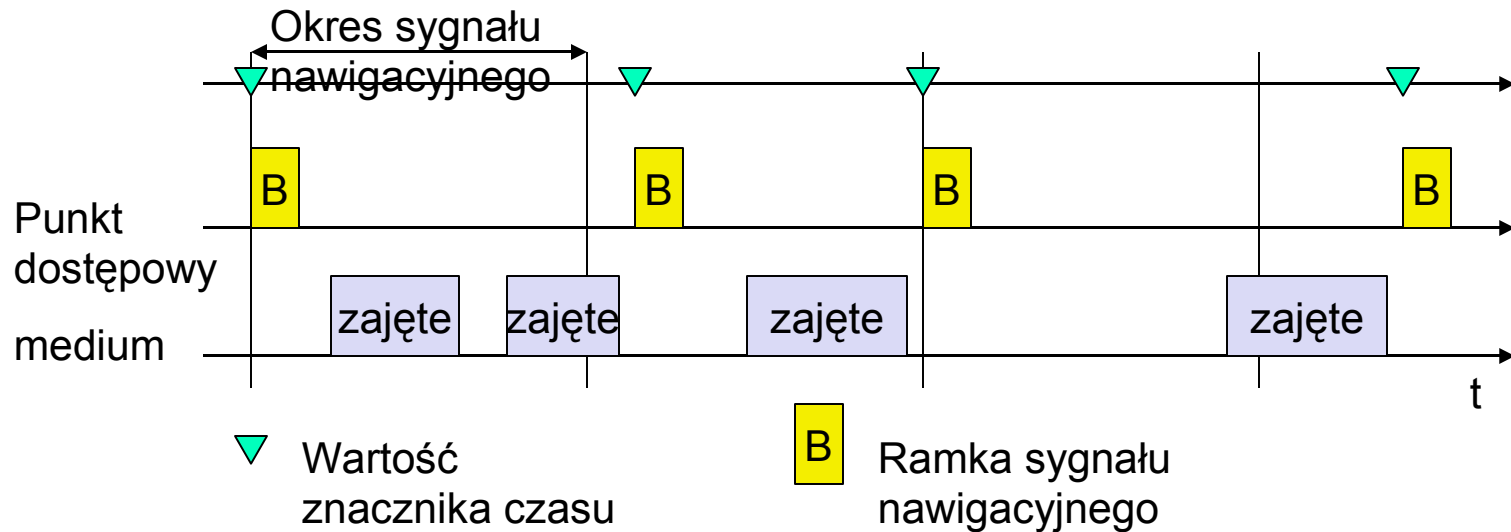


- ❑ Synchronizacja
 - Próbuj znaleźć sieć LAN, próbuj pozostać w sieci LAN
 - Zegarek, itd.
- ❑ Zarządzanie energią
 - Tryb hibernacji bez tracenia komunikatów
 - Okresy snu, buforowania ramek, pomiarów ruchu
- ❑ Asocjacja/Ponowna asocjacja
 - Integracja w sieci LAN
 - roaming, czyli zmiana sieci przez zmianę punktu dostępowego
 - scanning, czyli aktywne poszukiwanie sieci
- ❑ MIB - Management Information Base
 - Baza danych służących do zarządzania siecią

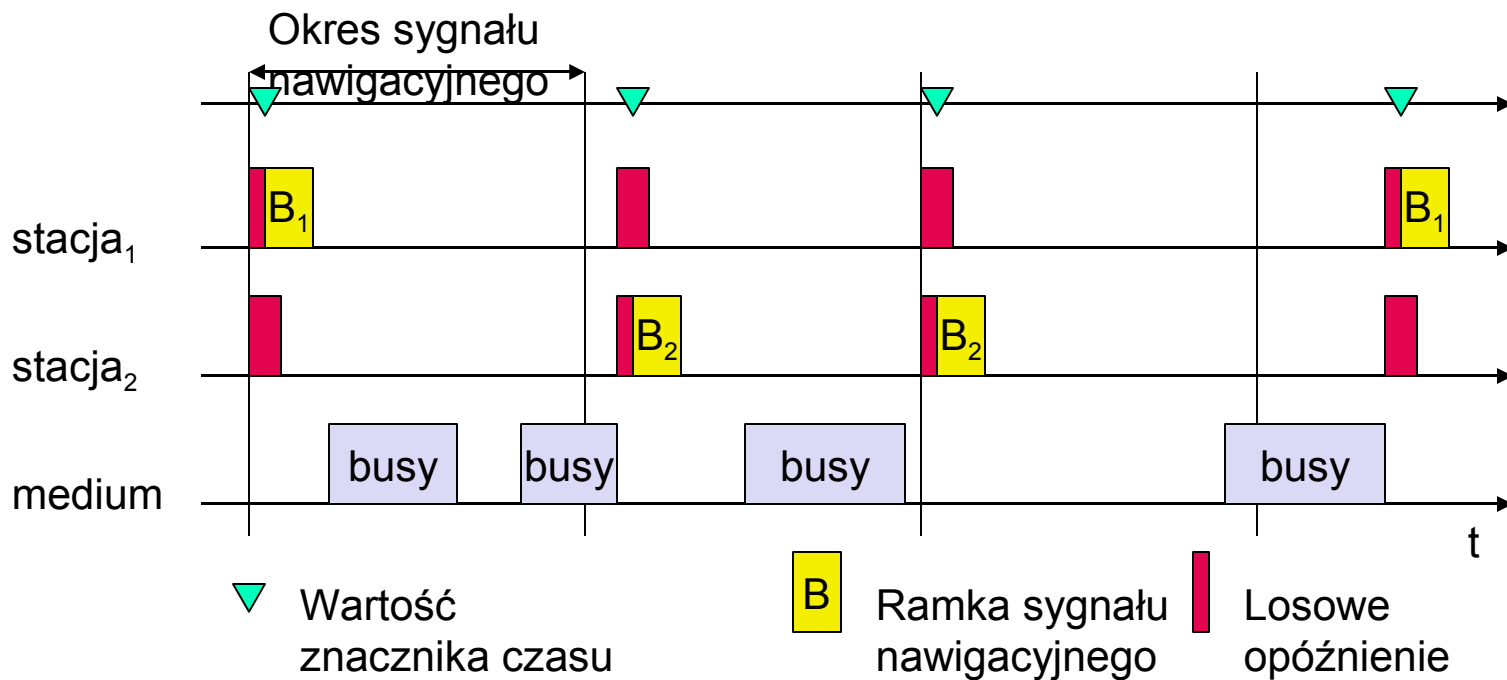


Synchronizacja (w sieci z infrastrukturą)

- Sygnał nawigacyjny (beacon)
 - Nadawany ciągle przez punkt dostępowy



Synchronizacja (w sieci ad-hoc)

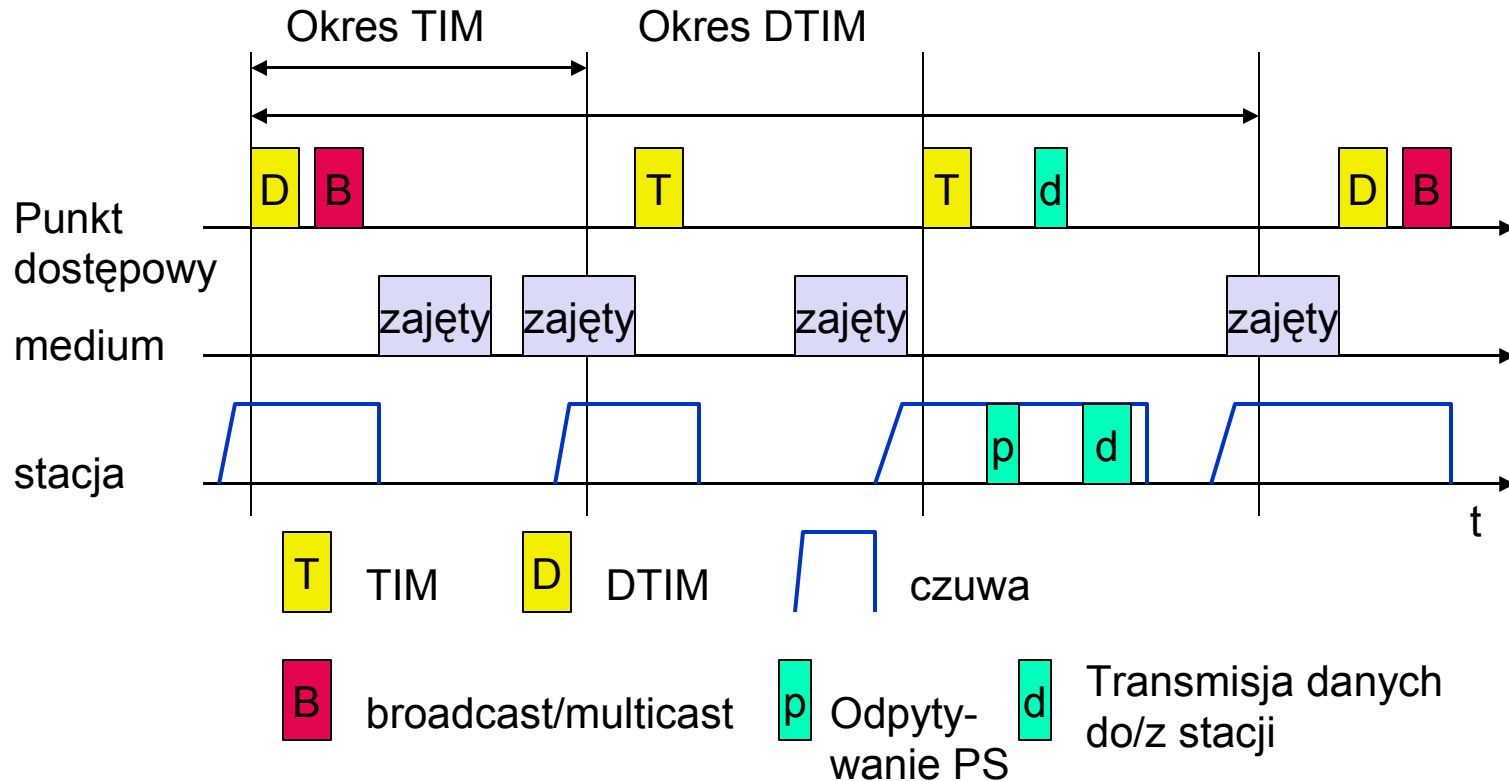


Zarządzanie energią

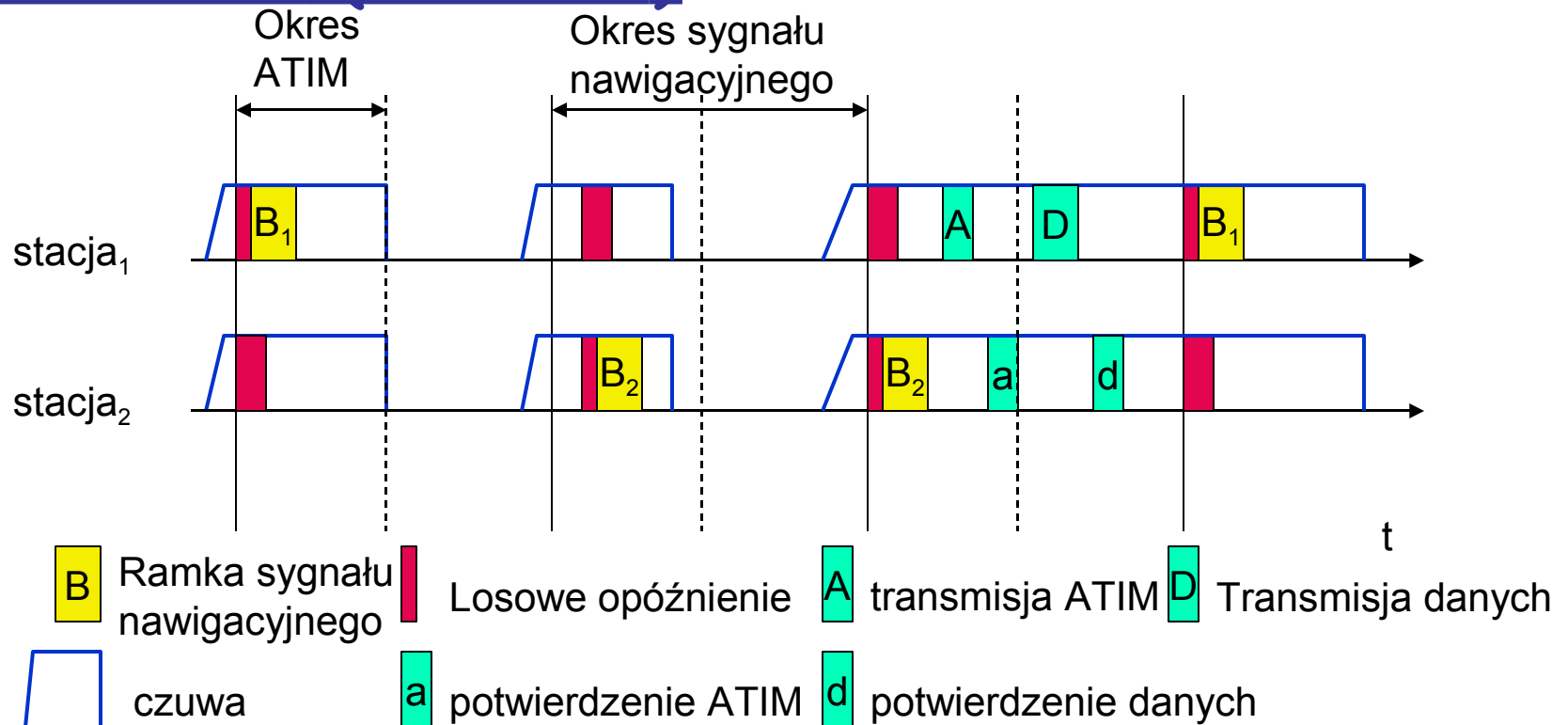


- ❑ Pomysł: wyłączyć nadajnik-odbiorcę, jeśli nie jest potrzebny
 - Ang. *Transceiver* = nadajnik-odbiorca
- ❑ Stany stacji: sen i czuwanie
- ❑ Timing Synchronization Function (TSF)
 - Stacje budzą się w tym samym czasie
- ❑ Infrastruktura
 - Traffic Indication Map (TIM)
 - Lista odbiorców unicast, wysyłana przez AP
 - Delivery Traffic Indication Map (DTIM)
 - Lista odbiorców broadcast/multicast, wysyłana przez AP
- ❑ Ad-hoc
 - Ad-hoc Traffic Indication Map (ATIM)
 - Ogłoszenia odbiorcy przez stacje buforujące ramki
 - Bardziej złożone - nie ma centralnego AP
 - Kolizje ramek ATIMs są możliwe (skalowalność?)

Zarządzanie energią przez okresy czuwania (infrastruktura)



Zarządzanie energią przez okresy czuwania (ad-hoc)



802.11 - Roaming



- ❑ Brak połączenia lub złe połączenie? Wykonaj:
- ❑ Skanowanie
 - Skanuj otoczenie, czyli nasłuchuj sygnałów nawigacyjnych lub wysyłaj próbne ramki i czekaj na odpowiedź
- ❑ Żądanie ponownej asocjacji
 - Stacja wysyła żądanie do nowego punktu dostępowego AP
- ❑ Odpowiedź na żądanie asocjacji
 - sukces: AP odpowiedział, stacja bieżę udział w jego sieci
 - porażka: stacja kontynuuje skanowanie
- ❑ AP akceptuje żądanie asocjacji
 - Informuje system dystrybucji o nowej stacji
 - System dystrybucji aktualizuje bazę danych (n.p., informacje lokalizacyjne)
 - zwykle, system dystrybucji informuje stary AP, który może zwolnić zasoby

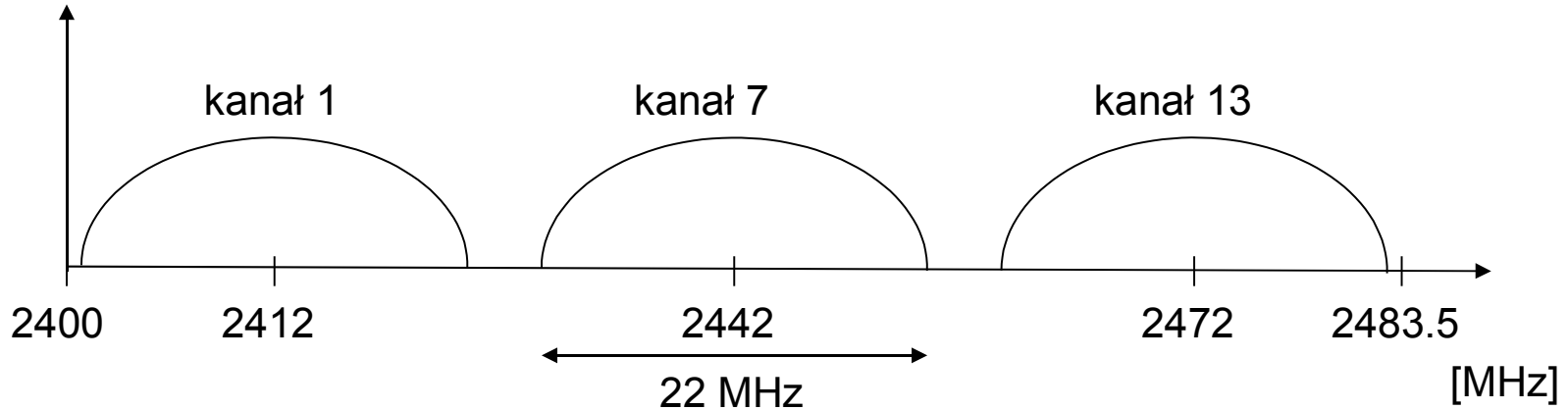
WLAN: IEEE 802.11b



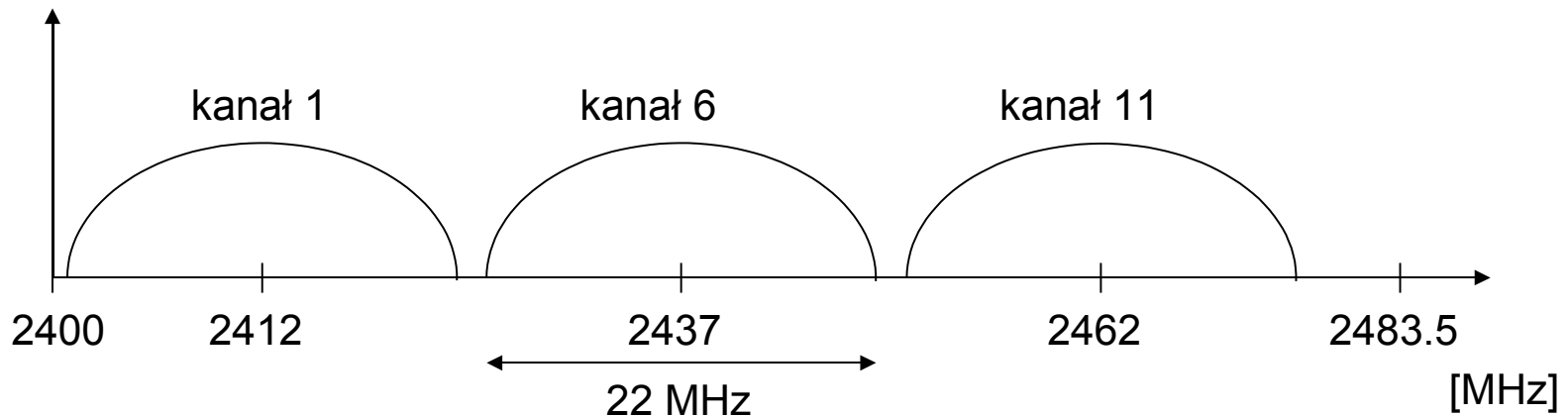
- ❑ Co nowego?
 - Definiuje nową warstwę PHY. Wszystkie protokoły MAC, zarządzania pozostają te same
 - Przepustowość danych użytkownika maks. około. 6 Mb/s
- ❑ Częstotliwości
 - Używa częstotliwości w wolnym paśmie ISM 2.4 GHz
- ❑ Ochrona informacji
 - Ograniczona, mało bezpieczny WEP, SSID
- ❑ Dostępność
 - Wiele produktów, producentów
- ❑ Specjalne zalety/Wady
 - Zalety: wiele zainstalowanych systemów, wiele doświadczenia, dostępne na całym świecie, wolne pasmo ISM, wielu producentów, zintegrowane z komputerami przenośnymi, proste
 - Wady: duże zakłócenia w paśmie ISM, brak gwarancji jakości, wolne

Wybór kanału (bez nakładania)

Europa (ETSI)



USA (FCC)/Kanada (IC)

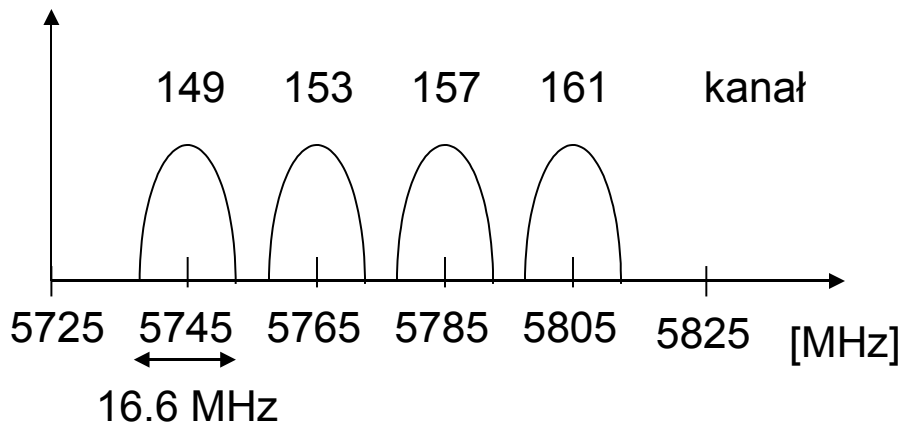
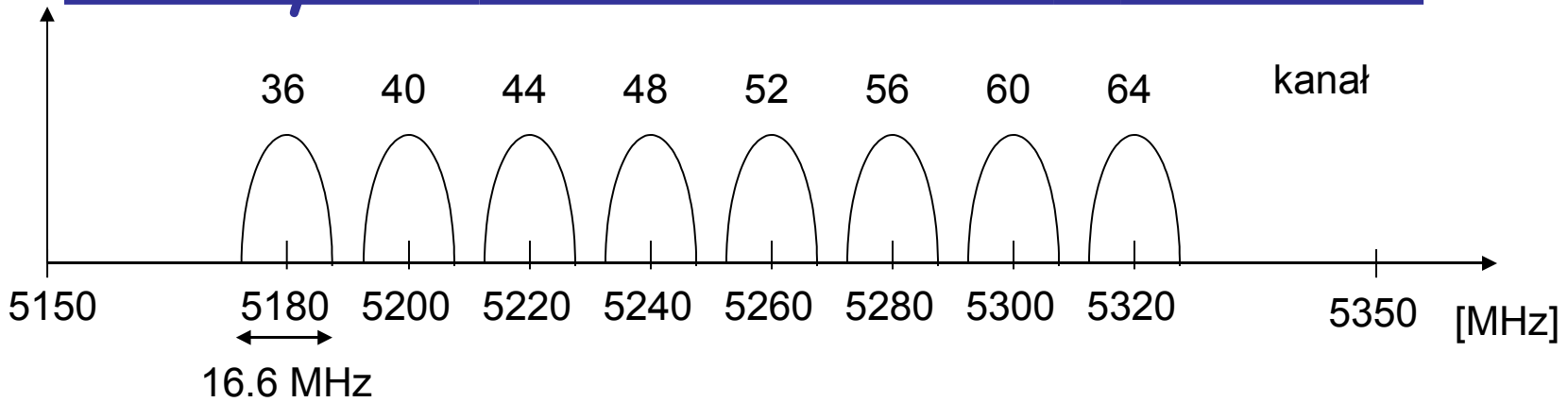


WLAN: IEEE 802.11a



- ❑ Częstotliwość
 - USA 5 GHz: wolne pasmo ISM 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz
- ❑ Multipleksacja: Orthogonal FDM (nowa forma FDM)
- ❑ Czas nawiązywania połączenia
 - Bezpołączeniowe/zawsze włączone
- ❑ Ochrona informacji
 - Ograniczona, mało bezpieczny WEP, SSID
- ❑ Dostępność
 - Kilka produktów i producentów
- ❑ Jakość usług
 - Typu best-effort (podobnie jak we wszystkich produktach 802.11)
- ❑ Specjalne zalety/Wady
 - Zalety: wolne pasmo ISM, dostępne, proste, używa pasma 5 GHz, w którym jest mniej zakłóceń
 - Wady: bardziej wrażliwe na przeszkody z powodu wyższej częstotliwości, brak QoS

Kanały dla 802.11a / USA U-NII



centralna częstotliwość =
 $5000 + 5 \cdot \text{numer kanału}$ [MHz]



WLAN: IEEE 802.11g

- ❑ Co nowego?
 - Definiuje nową warstwę PHY. Wszystkie protokoły MAC, zarządzania pozostają te same
 - Przepustowość danych maks. 54 Mb/s
 - Nowa modulacja, kody nadmiarowe, oraz OFDM - jak w 80.11a
- ❑ Częstotliwości
 - Używa częstotliwości w wolnym paśmie ISM 2.4 GHz - takie same, jak 802.11b
- ❑ Dostępność
 - Wiele produktów, producentów
- ❑ Specjalne zalety/Wady
 - Zalety: wiele zainstalowanych systemów, wiele doświadczenia, dostępne na całym świecie, wolne pasmo ISM, wielu producentów, zintegrowane z komputerami przenośnymi, proste
 - Wady: duże zakłócenia w paśmie ISM, brak gwarancji jakości



Przyszłość WLAN

- ❑ Ochrona informacji: 802.11i
 - Istniejący standard - mało wdrożeń
- ❑ Nowy standard ochrony informacji: 802.11w
 - Poprawa bezpieczeństwa ramek sterujących w warstwie MAC
- ❑ Przepustowość: 802.11n:
 - 540 Mb/s!
 - Pasma to samo, co 802.11b/g: 2.4 GHz !
 - Prawdopodobne zakończenie prac: 2007 rok
 - Pierwsze urządzenia: 2006 rok (Linksys, D-link, Netgear, Belkin)

ETSI - HIPERLAN

- ❑ Bezprzewodowy LAN obsługujący priorytety i czas życia ramek
- ❑ Standard ETSI
 - Standard Europejski
 - Rozszerzenie standardów sieci lokalnych
 - Od początku integruje usługi dla aplikacji wrażliwych na opóźnienia
- ❑ Rodzina HIPERLAN
 - jeden standard nie spełnia wszystkich wymagań:
 - zasięgu, przepustowości, jakości usług
 - ograniczeń komercyjnych
 - HIPERLAN 1 jest standardem od 1996 roku - nie ma produktów!

Przegląd: oryginalna rodzina protokołów HIPERLAN

	HIPERLAN1	HIPERLAN2	HIPERLAN3	HIPERLAN4
Application	wireless LAN	access to ATM fixed networks	wireless local loop	point-to-point wireless ATM connections
Frequency	5.153 GHz			17.2-17.3 GHz
Topology	decentralized ad-hoc infrastructure	cellular, centralized	point-to-multipoint	point-to-point
Antenna	omni-directional		directional	
Range	50m	50-100m	500m	150m
QoS	statistical	ATM traffic classes (NBR, CBR, ABR, UBR)		
Mobility	<10m/s		stationary	
Interface	conventional LAN	ATM networks		
Rate	23.5 Mbit/s	>20 Mbit/s		155 Mbit/s
Power conservation	yes		not necessary	

HIPERLAN 1 nigdy nie był produkowany, pozostałe standardy zostały zmodyfikowane i zmieniły nazwy!

HIPERLAN 1

- Wiele terminali może chcieć nadawać z tym samym priorytetem
 - faza rywalizacji
 - Węzeł z priorytetem p słucha kanału przez p ramek
 - Jeśli kanał jest wolny przez cały okres p ramek, węzeł potwierdza swój priorytet przez transmisję ciągu bitów (11111010100010011100000110010110, wysoka przepustowość)
 - Węzeł zaprzestaje próby nadawania, jeśli usłyszy sygnały w kanale
 - Faza rywalizacji kończy się, gdy węzeł potwierdzi swój priorytet
 - transmisja danych
 - zwycięzca wysyła dane (choć nadal istnieje niewielka szansa kolizji)
 - do synchronizacji służy ostatnia transmisja danych

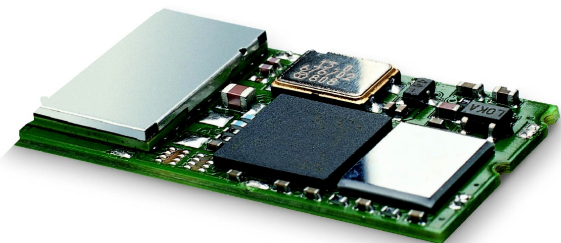
Trochę historii: Czemu bezprzewodowy ATM?

- ❑ gładkie połączenie z przewodowym ATM, sieć o wysokiej wydajności, oferująca różne rodzaje zintegrowanych usług
- ❑ Sieci ATM skalują się od sieci LAN do WAN, a mobilność jest potrzebna zarówno w lokalnych, jak i rozległych sieciach
- ❑ Oferuje QoS dla komunikacji multimedialnej
- ❑ Połączenie sieci ATM i komunikacji mobilnych, bezprzewodowych urządzeń jest naturalne
- ❑ Bezprzewodowe ATM jest przydatne z punktu widzenia operatora sieci telekomunikacyjnej
- ❑ **Problem: bardzo duża złożoność - nie ma produktów**

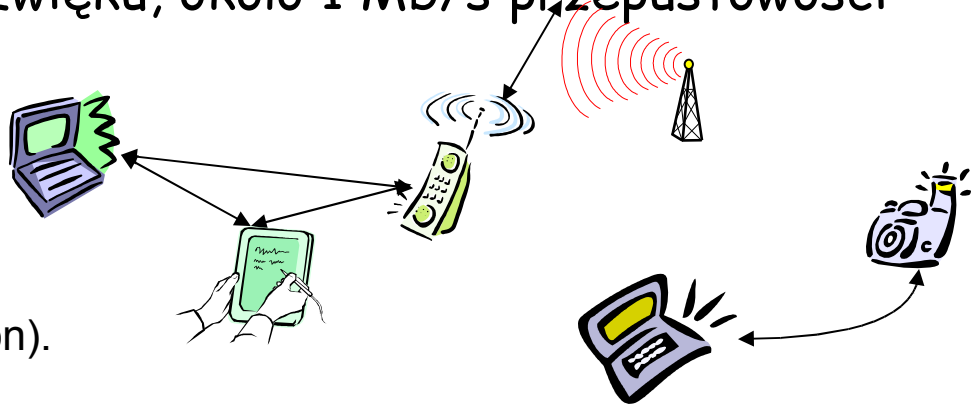
Bluetooth

□ Koncepcja

- Uniwersalna łączność radiowa dla połączeń ad-hoc
- Połączenie komputerów z urządzeniami peryferyjnymi, przenośnymi, klasy PDA, telefonami komórkowymi - zastępuje IrDA
- Wbudowane w inne urządzenia, cel: 5€/device (2002: 50€/USB Bluetooth)
- Krótki zasięg (do 10 m), niski pobór mocy, wolne pasmo ISM 2.45 GHz
- Transmisja danych i dźwięku, około 1 Mb/s przepustowości



Jeden z pierwszych modułów (Ericsson).



Bluetooth



(było:  Bluetooth™)

□ Historia

- 1994: Projekt "MC-link" firmy Ericsson
- Zmiana nazwy: Bluetooth po królu Haraldzie "Blåtand" Gormsen [syn Gorma], Królu Danii w 10-tym wieku
- 1998: założenie Bluetooth SIG (Special Interest Group), www.bluetooth.org
- 1999: ustawienie kamienia runicznego w Ericsson/Lund ;-)
- 2001: pierwsze produkty na rynku masowym, opublikowana wersja 1.1 specyfikacji

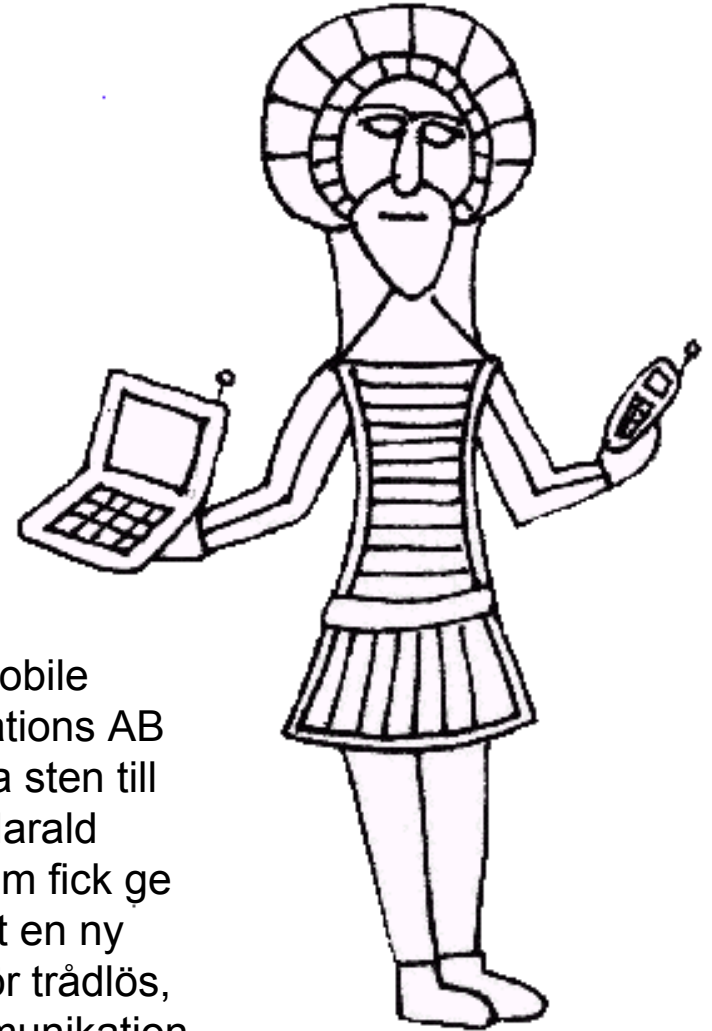
□ Special Interest Group

- Członkowie założyciele: Ericsson, Intel, IBM, Nokia, Toshiba
- Dodani promotorzy: 3Com, Agere (poprzednio: Lucent), Microsoft, Motorola
- ponad 2500 członków
- Wspólna specyfikacja i certyfikacja produktów

Historia i hi-tech...



1999:
Ericsson mobile
communications AB
reste denna sten till
minne av Harald
Blåtand, som fick ge
sitt namn åt en ny
teknologi för trådlös,
mobil kommunikation.



...i prawdziwy kamień runiczny



Położony w Jelling, Dania, ustawiony przez Króla Haralda “Blåtand” dla upamiętnienia jego rodziców. Kamień ma trzy strony – jedna strona pokazuje obraz Chrystusa.

Inskrypcja na kamieniu:

"Harald król wykonał ten wspaniały pomnik ku pamięci Gorma, swojego ojca, i Thyry, swojej matki. Ten Harald który podbił całą Danię i norwegię i nawrócił Duńczyków na Chrześcijaństwo."

A propos: Blåtand oznacza “ciemnej karnacji” (a nie z niebieskim zębem...)



Tak mogły wyglądać oryginalne kolory kamienia.



Krótką charakterystyka Bluetooth

- ❑ Technologia sieci bezprzewodowych o małej mocy, małym zasięgu
 - 10-100 metrów
- ❑ bezkierunkowy
 - nie to samo co podczerwień
- ❑ łączy małe urządzenia
- ❑ Używa nie licencjonowanego pasma 2.4-2.5 GHz
- ❑ do 721 kb/s
- ❑ Zakłócenia za strony bezprzewodowych sieci LAN, telefonów bezprzewodowych, mikrofalówek:
 - pomaga przeskakiwanie po częstotliwościach
- ❑ Protokół MAC udostępnia:
 - naprawę błędów
 - ARQ
- ❑ Każdy węzeł ma 12-bitowy adres

Charakterystyka bardziej szczegółowa

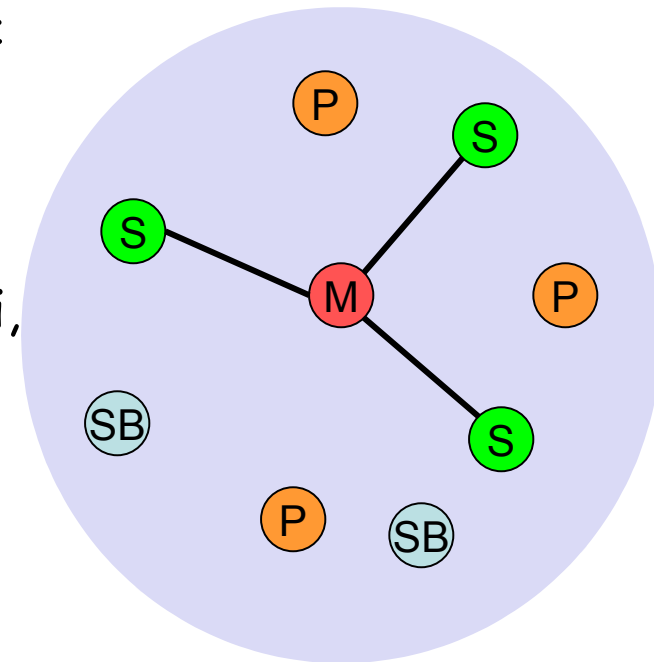


- ❑ Pasma ISM 2.4 GHz, 79 (23) kanałów RF, oddzielenie częstotliwości nośnych o 1 MHz
- ❑ FHSS oraz TDD
 - Przeskakiwanie po częstotliwościach z częstością 1600 zmian na sekundę
 - Pseudolosowy ciąg częstotliwości, ustalany przez kontrolera ("master")
 - *Time division duplex* dla oddzielenia nadawania i odbierania
- ❑ Łącze głosowe - SCO (Synchronous Connection Oriented)
 - Kody nadmiarowe (FEC, forward error correction), brak retransmisji, 64 kb/s dwupłask, punkt-punkt, komutacja kanałów
- ❑ Łącze danych - ACL (Asynchronous ConnectionLess)
 - Asynchroniczne, szybkie potwierdzenia, punkt-wielopunkt, do 433.9 kb/s symetrycznie lub 723.2/57.6 kb/s asymetrycznie, komutacja pakietów
- ❑ Topologia
 - Nakładające się na siebie pikosieci (gwiazdy) tworzą "scatternet"

Pikosieć (ang. Piconet)



- ❑ Zbiór urządzeń połączonych w sposób ad-hoc
- ❑ Jedno urządzenie pełni rolę koordynatora ("master"), pozostałe są podwładnymi ("slave") przez czas istnienia pikosieci
- ❑ Koordinator ustala sekwencję częstotliwości, podwładni muszą się synchronizować
- ❑ Każda pikosieć ma niepowtarzalny ciąg częstotliwości
- ❑ Udział w pikosieci = synchronizacja z ciągiem częstotliwości
- ❑ Każda pikosieć ma **jednego koordynatora** o najwyżej 7 podwładnych jednocześnie (ponad 200 może być nieaktywnych, "parked")



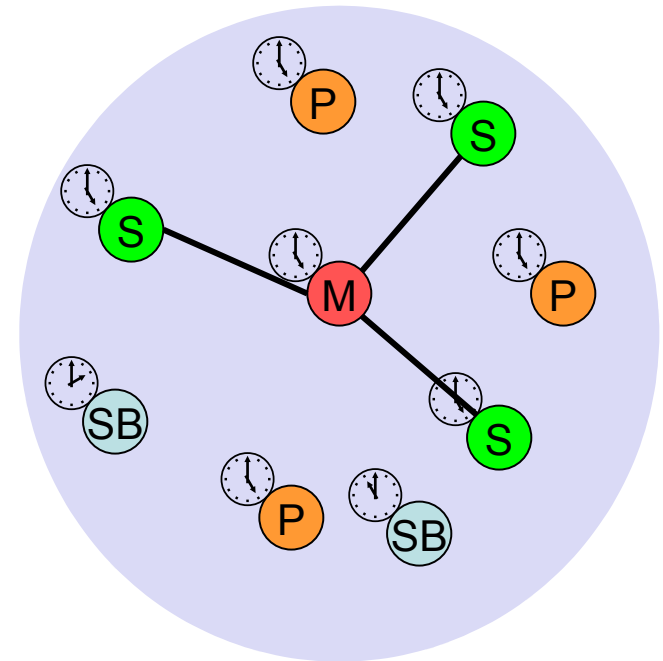
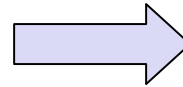
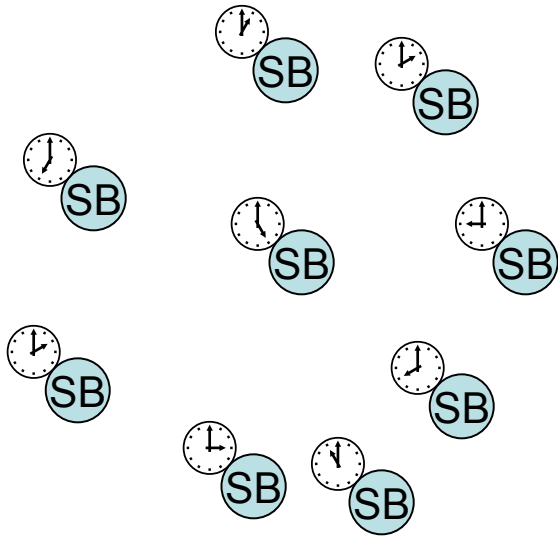
M=Master
S=Slave

P=Parked
SB=Standby

Tworzenie się pikosieci



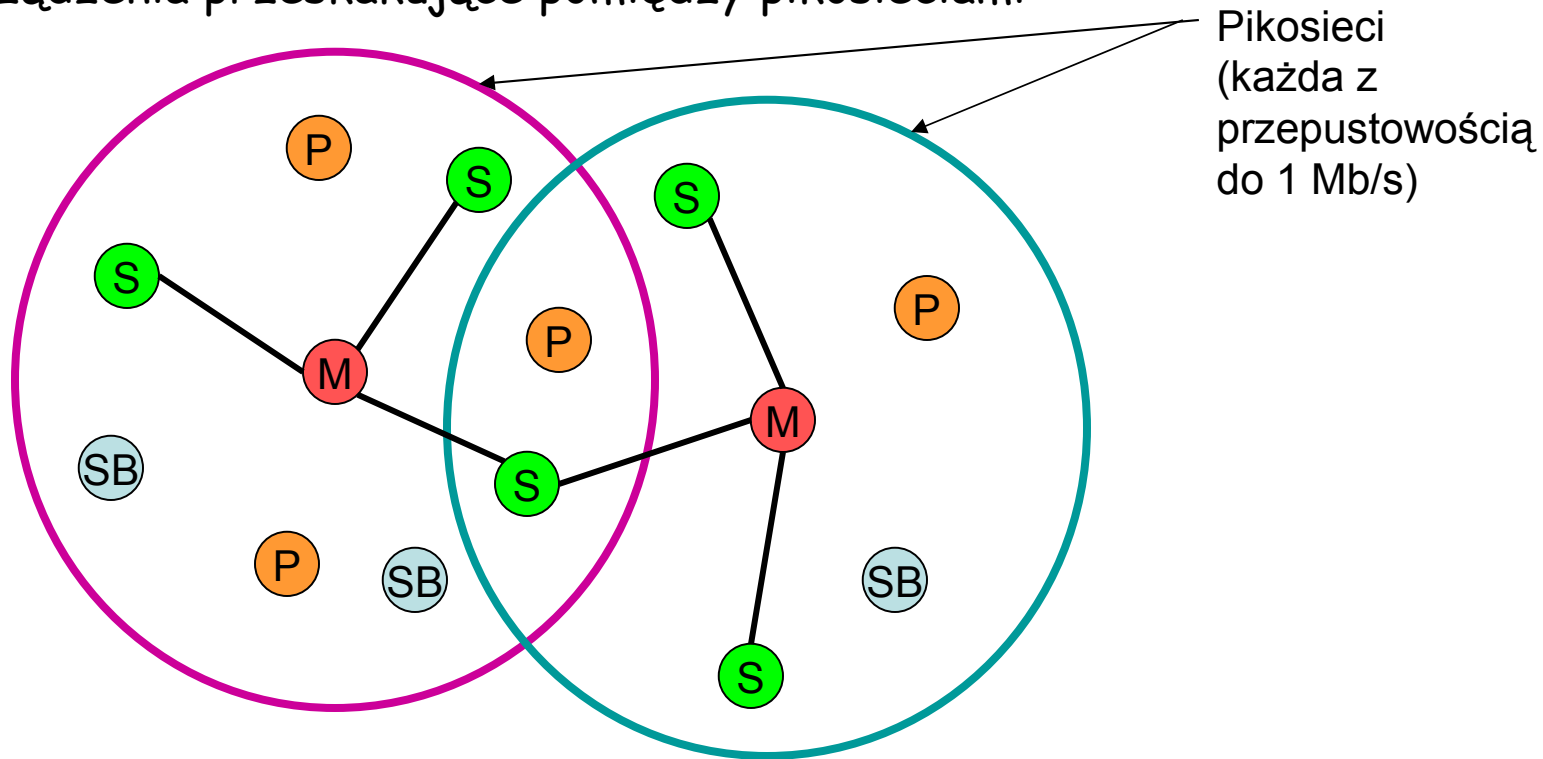
- Wszystkie urządzenia pikosieci zmieniają częstotliwości jednocześnie
 - Koordynator daje podwładnym swój czas zegara i identyfikator ID
 - Ciąg częstotliwości: ustalany przez identyfikator ID (48 bitów, niepowtarzalny na całym świecie)
 - Okres zmian częstotliwości ustalany przez czas zegara
- Adresowanie
 - Active Member Address (AMA, 3 bit)
 - Parked Member Address (PMA, 8 bit)



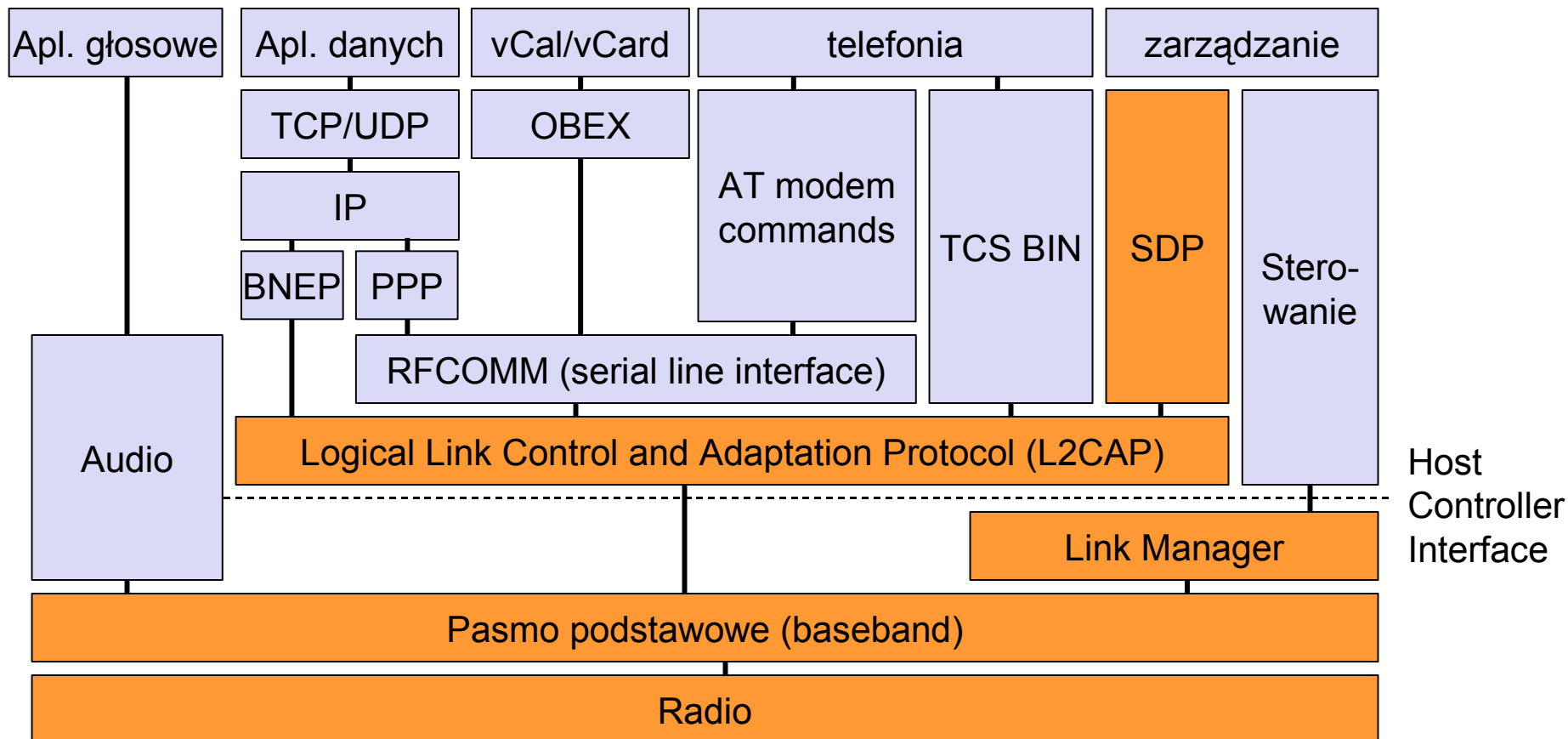
Scatternet



- Połączenie wielu nakładających się pikosieci poprzez wspólne urządzenia koordynujące lub podwładnych
 - Urządzenia mogą być podwładnymi w jednej pikosieci, a koordynatorami w drugiej
- Komunikacja pomiędzy pikosieciami
 - Urządzenia przeskakujące pomiędzy pikosieciami



Stos protokołów Bluetooth



AT: attention sequence

OBEX: object exchange

TCS BIN: telephony control protocol specification – binary

BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol

RFCOMM: radio frequency comm.

Warstwa radia: określa częstotliwości, modulację

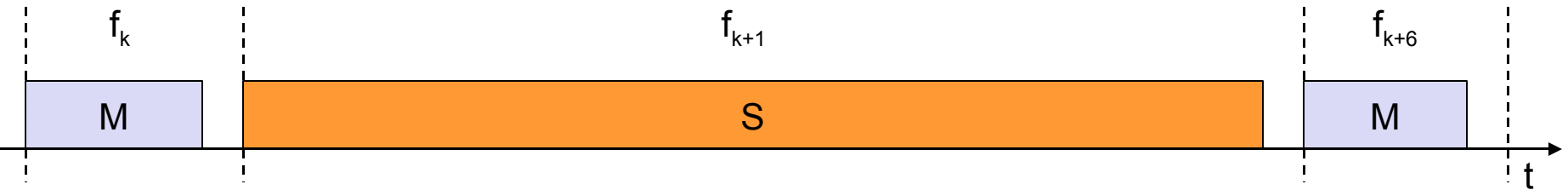
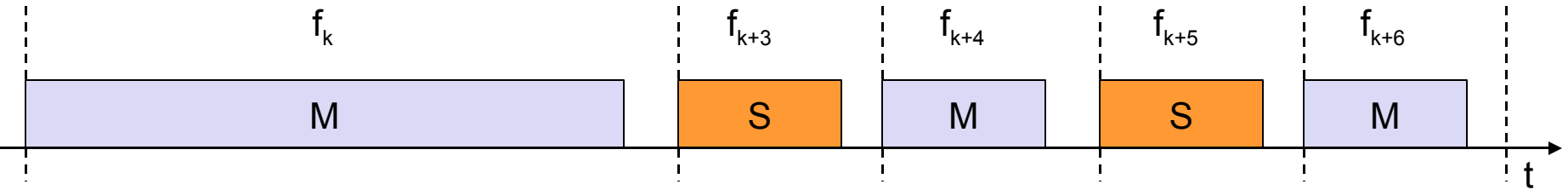
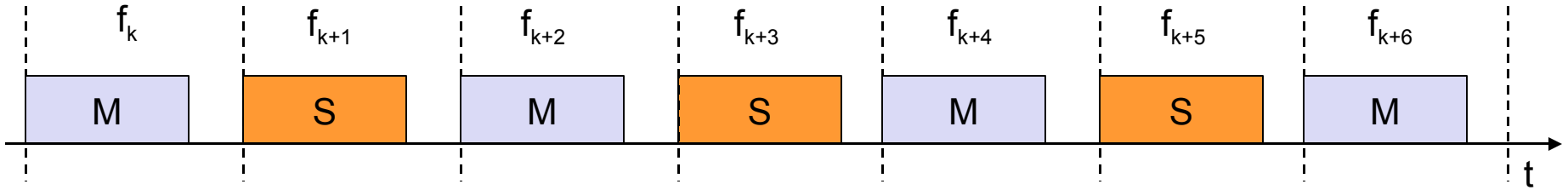
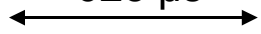


- ❑ Pasma ISM 2.4 GHz, 79 RF kanałów, kanałów RF, oddzielenie częstotliwości nośnych o 1 MHz
- ❑ FHSS oraz TDD
 - Przeskakiwanie po częstotliwościach z częstością 1600 zmian na sekundę
 - Pseudolosowy ciąg częstotliwości, ustalany przez kontrolera ("master")
 - *Time division duplex* dla oddzielenia nadawania i odbierania



Warstwa pasma podstawowego

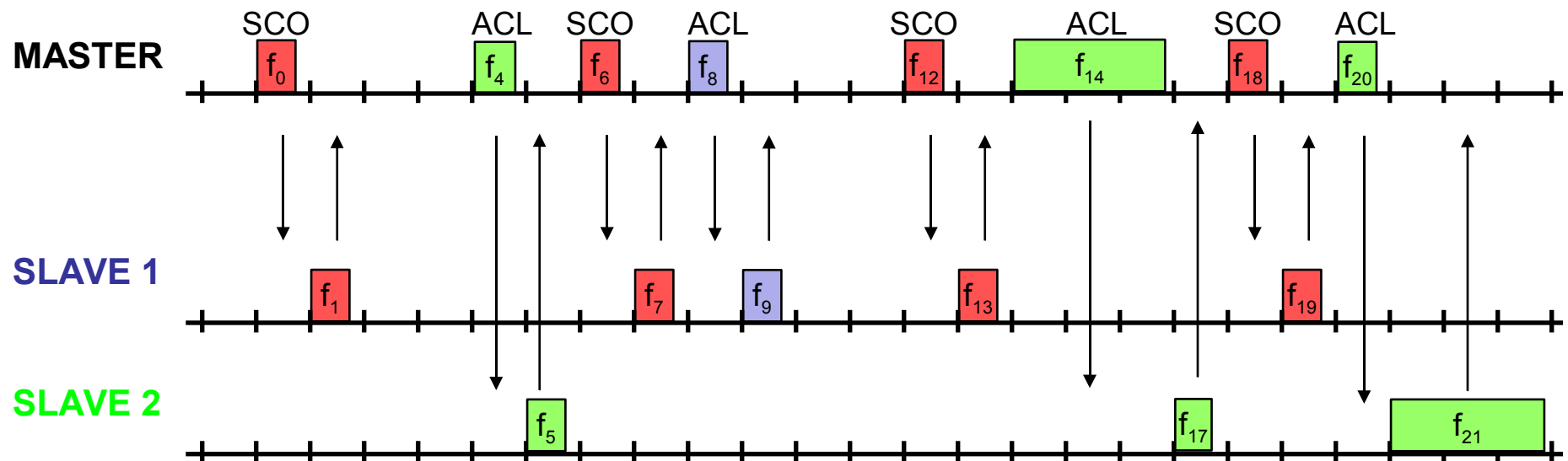
625 μ s



Rodzaje łączy pasma podstawowego



- ❑ Transmisja pakietów w oparciu o odpytywanie (TDD)
- ❑ SCO (Synchronous Connection Oriented) - Głos
 - Okresowe przydzielanie jednej ramki, 64 kb/s full-duplex, punkt-punkt
- ❑ ACL (Asynchronous ConnectionLess) - Dane
 - Zmienna długość ramki (1,3,5), asymetryczna przepustowość, punkt-wielopunkt

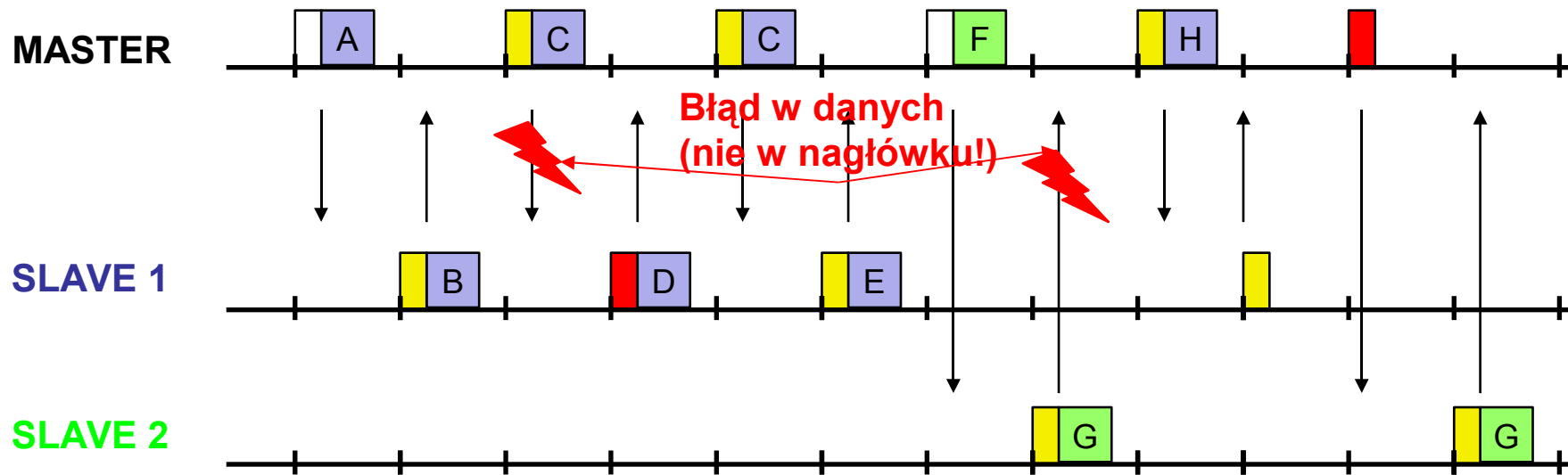


Niezawodność

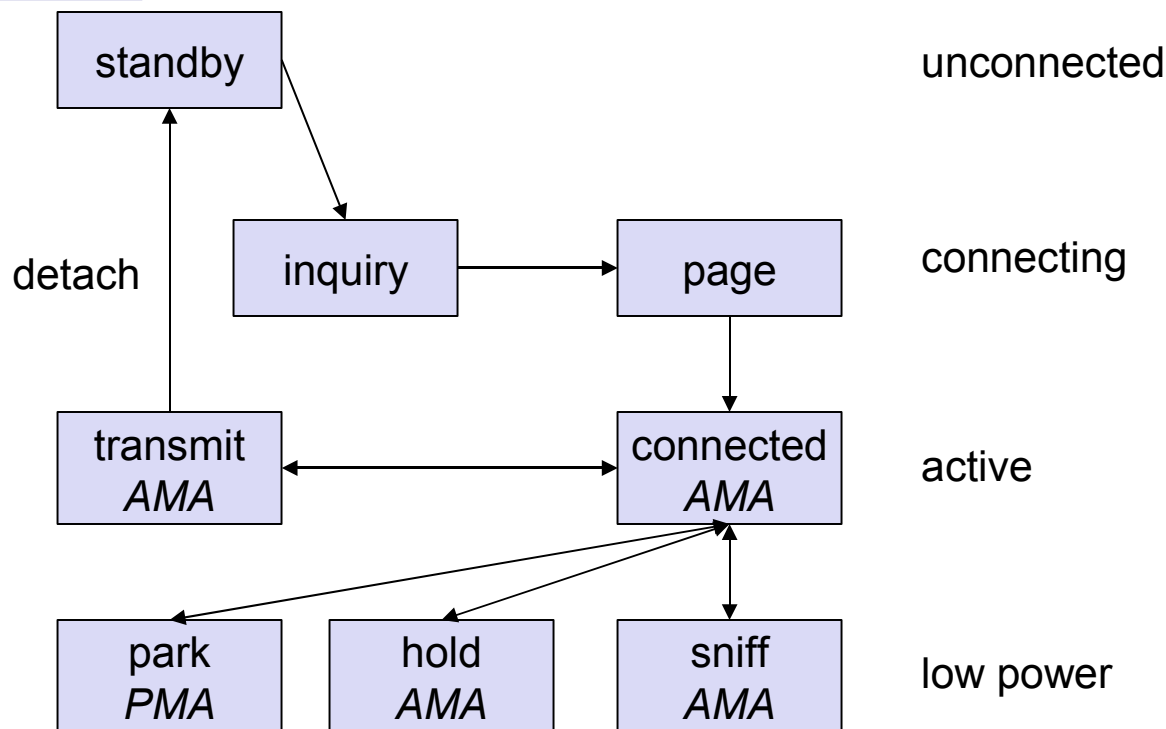


- Wolne przeskakiwanie po częstotliwościach według wzorca ustalonego przez koordynatora
 - Chroni przed zakłóceniami na niektórych częstotliwościach
 - Oddziela od innych pikosieci (FH-CDMA)
- Naprawa błędów:
 - wysyłamy 3 kopie każdego pakietu, odbiorca podejmuje decyzję większościową
- Retransmisje
 - Tylko tryb asynchroniczny, bardzo szybkie

■ NAK ■ ACK



Stany pasma podstawowego urządzenia Bluetooth



Standby: nie rób nic

Inquire: szukaj innych urządzeń

Page: połącz się z konkretnym urządzeniem

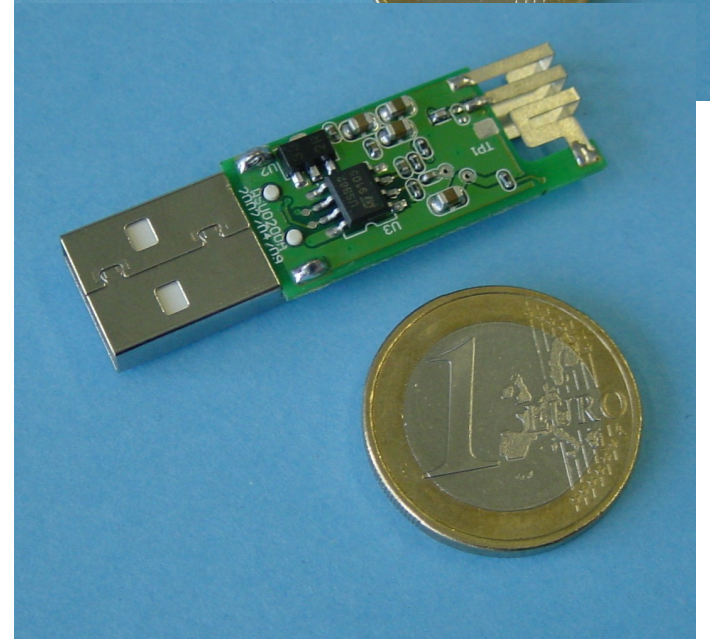
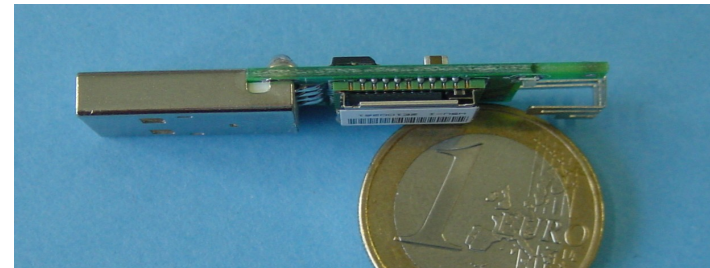
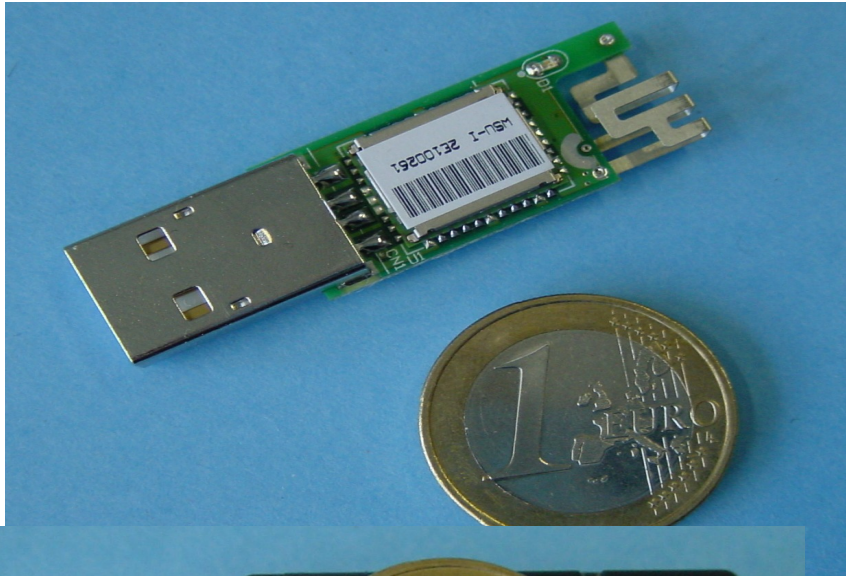
Connected: bierz udział w pikosieci

Park: oddaj *AMA*, pobierz *PMA*

Sniff: słuchaj okresowo, nie każdej ramki

Hold: zatrzymaj *ACL*, *SCO* dalej możliwe, możliwe wzięcie udziału w innej pikosieci

Przykład: Adapter Bluetooth/USB (2002 rok: 50€)





SDP - Service Discovery Protocol

- Protokół zapytania/odpowiedzi dla znajdowania usług
 - Poszukiwanie i eksploracja usług w sąsiedztwie radiowym
 - Dostosowany do bardzo zmiennego środowiska
 - Definiuje tylko znajdowanie, a nie wykorzystanie usług
 - Utrzymuje „cache” odkrytych usług
 - Stopniowe odkrywanie usług



IEEE 802.15

- ❑ WPAN: IEEE 802.15-1 - Bluetooth
 - Standardyzacja niższych warstw Bluetooth

- ❑ WPAN: IEEE 802.15.2 - rozwój 1
 - Współistnienie Wireless Personal Area Networks (802.15) i Wireless Local Area Networks (802.11), określa wzajemne zakłócanie

- ❑ 802.15-3: Wysoka przepustowość
 - Standard sieci WPAN o wysokiej przepustowości (20Mb/s lub większej), wciąż o małym poborze mocy/koszcie
 - Protokół QoS
 - Sieć ad-hoc
 - Ochrona informacji
 - Mały pobór mocy
 - Mały koszt
 - Ma na celu zaspokoić oczekiwania konsumentów dotyczących multimedialnej komunikacji bezprzewodowej

Ochrona informacji w bezprzewodowych sieciach LAN

- ❑ Proste formy zabezpieczeń
- ❑ Protokoły
 - Poufność
 - WiFi: WEP, WPA, WPA2/802.11i
 - Bluetooth
 - Uwierzytelnienie
 - WiFi: WEP, WPA-PSK, WPA-EAP
 - Bluetooth
- ❑ Naruszenia bezpieczeństwa sieci
 - Wardriving, Warflying, Warchalking...
 - Wrogie punkty dostępowe
 - Zagrożenia WiFi, Bluetooth
 - Metody ochrony

Sieci bezprzewodowe i zagrożenia

- ❑ Bezprzewodowe słuchawki...
- ❑ Dostęp do WWW na lotnisku lub w galerii...
- ❑ Praca w systemie "hot desk"...
- ❑ Czytanie poczty na organizerze...
- ❑ ... wygoda, czy początek katastrofy??

Bilans sił

- ❑ Napastnik ma większą antenę i silniejszy sygnał...
- ❑ Napastnik ma szybszy komputer (lub cały klaster)...
- ❑ Napastnik wybiera czas i miejsce ataku...
- ❑ Napastnik jest mobilny, cel - niekoniecznie...
- ❑ Napastnik może nasłuchiwać dowolnie długo, będąc niezauważonym...

Proste formy zabezpieczeń

- ❑ Filtrowanie adresów MAC
 - adres MAC łatwo jest zmienić
 - bezwartościowe
- ❑ "Zamknięte" sieci
 - SSID nie jest rozgłaszane przez punkt dostępowy
 - ale jest zawarte w innych ramkach
- ❑ Wyłączanie DHCP
 - nie marnujcie na to czasu

Protokoły - poufność: WEP



- 802.11 - **Wireless Equivalent Privacy**
 - Szyfr: RC4
 - oparty na operacji XOR danych ze strumieniem kluczy szyfrujących
 - Klucze szyfrujące generowane na podstawie klucza WEP oraz wektora inicjalizującego (IV)
 - Manualna dystrybucja kluczy
 - Suma kontrolna: CRC-32
 - Algorytm wybrano z powodów:
 - wydajności
 - ograniczeń eksportowych USA

Protokoły - poufność: WEP



K – klucz WEP

IV – wektor inicjujący



Protokoły - poufność: WEP



□ 802.11 - WEP: ataki

○ Kryptoanaliza:

- AirSnort, 2001: szuka "słabych" wektorów IV, pozwalających odgadnąć klucz WEP
- chopper -> aircrack, WepLab, 2004: narzędzie statystyczne. Potrzebuje tylko 200.000 pakietów

○ Ataki słownikowe: WepAttack

○ Ataki powtórzeniowe (ang. *replay attacks*)

- Cel: zebranie danych do kryptoanalizy lub ataku słownikowego
- WEP nie ma ochrony przed tym atakiem. Nie trzeba odszyfrować pakietu, żeby odgadnąć jego rodzaj po długości i adresie odbiorcy
- aireplay

○ Ataki na klucze szyfrujące

- zamiast odgadywać klucz WEP, poznać klucze szyfrujące - wystarczy, by wysłać własne pakiety
- WEPWedgie

Klasy ataków na IEEE 802.11 (WEP)

- ❑ Atak wykorzystujący ponowne użycie IV
- ❑ Atak ze znanym tekstem jawnym
- ❑ Atak z częściowo znanym tekstem jawnym
- ❑ Atak słownikowy
- ❑ Atak wykorzystujące słabości algorytmu RC4
- ❑ Podszywanie się
- ❑ Odmowa usługi (denial of service)

Ponowne użycie IV

- ❑ Autorzy: Borisov, Goldberg, Wagner
 - Atak teoretyczny
- ❑ Wykorzystanie własności działania XOR (suma modulo 2):
- ❑ - $X \text{ XOR } X = [0,0,\dots]$, $Y \text{ XOR } [0,0,\dots] = Y$
- ❑ (IV,k) daje strumień klucza: $RC4(IV,k)$
 - Pierwszy szyfrogram: $C1 = M1 \text{ XOR } RC4(IV,k)$
 - Drugi szyfrogram: $C2 = M2 \text{ XOR } RC4(IV,k)$
 - $C1 \text{ XOR } C2 = M1 \text{ XOR } RC4(IV,k) \text{ XOR } M2 \text{ XOR } RC4(IV,k) = M1 \text{ XOR } M2$
- ❑ $M1, M2$ można przewidzieć
- ❑ dodatkowo: IV jest generowane za pomocą licznika, inkrementowanego co 1 i zerowany po każdym restarcie karty
- ❑ przestrzeń IV : 224
- ❑ wniosek dla wytwórców sprzętu: IV powinno być generowane losowo

Przeszukiwanie przestrzeni klucza

- ❑ Autor: Tim Newsham
 - Jeden z najefektywniejszych pod względem szybkości ataków
- ❑ Atakujący posiada zestaw kluczy:
 - przechwycenie pakietu 802.11
 - deszyfrowanie wybranym kluczem pola użytkowego pakietu
 - zliczenie sumy kontrolnej
 - jeśli suma zgadza się: odszyfrowujemy pole użytkowe następnego pakietu
 - jeśli znowu się zgadza - mamy klucz!
- ❑ Atak skuteczny na urządzenie IEEE 802.11 mające generatory kluczy bazujące na hasłach: redukcja przestrzeni klucza z 240 do 221
- ❑ W praktyce: zestaw kluczy= słownik (atak słownikowy)
- ❑ Wniosek dla użytkowników WLAN: nie używać kluczy bazujących na hasłach

Atak na słabe klucze RC4

- ❑ Autorzy: Fluhrer, Mantin, Shamir
 - najczęściej implementowany atak (AirSnort, WEPcrack)
- ❑ Atak niezależny od długości klucza RC4
- ❑ Atak na IV postaci: $(A + 3, N - 1, X)$
- ❑ Stwierdzenie czy IV jest słabe zaraz po kroku KSA algorytmu RC4: $X = S\{B + 3}[1] < B + 3, X + S\{B + 3}[X] = B + 3$
- ❑ atak z wykorzystaniem znajomości pierwszego bajtu strumienia klucza - na którym ukazuje się fragment współdzielonego klucza
- ❑ wykrywanie poszczególnych bajtów współdzielonego klucza poprzez „probabilistyczne głosowanie”
- ❑ (spóźnione) wnioski dla twórców standardu IEEE 802.11: pominąć pierwsze bajty strumienia klucza RC4 albo stosować klucze sesyjne
- ❑ wniosek dla wytwórców sprzętu: nie dopuszczać do użycia słabych IV albo stosować klucze sesyjne

Protokoły - poufność: WEP

□ 802.11 - WEP

- wniosek: nie używać?

□ Nie całkiem...

- WEP można złamać w pięć minut.
- Czemu nie zmieniać automatycznie klucza WEP co kilka minut?
- SecureWEP - rozwiązanie opracowane w PJWSTK



Protokoły - poufność: WPA

- 802.11 - **Wireless Protected Access**
 - Szyfr: RC4 !!
 - nowy protokół, TKIP, ale stary szyfr...
 - Większe klucze, wektory IV
 - używa wielu kluczy
 - Dynamiczna wymiana klucza co 10k
 - Jednorazowe wartości: uniemożliwiają ataki powtórzeniowe
 - Nowa suma kontrolna (Michael) zapewnia integralność



Protokoły - poufność: WPA2

- 802.11i (AES-CCMP)
 - uchwalone przez IETF w czerwcu, 2004
 - Szyfr: AES
 - Michael zastąpiono przez CCMP (algorytm *Message Authentication Code, MAC*)
- WPA2 zapewnia poufność...
 - jednak ma większe wymagania obliczeniowe
 - nadal możliwe jest podszywanie się pod adresy MAC, wysyłanie ramek sygnalizacyjnych, ataki DoS



Protokoły - poufność: Bluetooth

- Szyfr: E0
 - specjalnie zaprojektowany dla Bluetooth
 - klucze generowane dla każdej sesji
 - z klucza dla sesji, generowany jest klucz dla pakietu
 - w WEP, zbyt często używano tych samych kluczy dla różnych pakietów
 - Bezpośrednie ataki istnieją - ale są złożone obliczeniowo
 - oddzielne klucze do szyfrowania i uwierzytelnienia

Plan wykładu

- ❑ Wstęp: bezprzewodowe sieci lokalne (WLAN)
- ❑ Proste formy zabezpieczeń
- ❑ Protokoły
 - Poufność
 - WiFi: WEP, WPA, WPA2/802.11i
 - Bluetooth
 - Uwierzytelnienie
 - WiFi: WEP, WPA-PSK, WPA-EAP
 - Bluetooth
- ❑ Naruszenia bezpieczeństwa sieci
 - Wardriving, Warflying, Warchalking...
 - Wrogie punkty dostępowe
 - Zagrożenia WiFi, Bluetooth
 - Metody ochrony



Protokoły - uwierzytelnienie: WEP

□ Procedura challenge-response

- oparta na szyfrowaniu: trzeba udowodnić, że zna się wspólny klucz WEP
- dwustronna, symetryczna
- przy każdym uwierzytelnieniu, używany jest ten sam klucz

□ Możliwy atak na klucz szyfrujący

- wystarczy, by podszyć się pod ofiarę po wysłuchaniu początku procedury
- nie trzeba znać klucza WEP



Protokoły - uwierzytelnienie: WPA

□ Dwa rodzaje

○ Pre-Shared Key

- oparty na wspólnym kluczu (np. hasło)

○ Extensible Authentication Protocol

- uwierzytelnienie 802.1X
- oparte o uwierzytelnienie użytkowników, oraz certyfikat punktu dostępowego. Możliwy mechanizm: TLS. Wymagany serwer RADIUS
- może także użyć certyfikatów klientów: ochrona przed atakami słownikowymi



Protokoły - uwierzytelnienie: Bluetooth

- ❑ Oparte o wspólny sekret, challenge-response
 - tzw. klucz łącza (ang. *link key*)
 - dwa rodzaje:
 - unit key: dla wszystkich połączeń
 - combination key: dla jednego połączenia
 - oparty o szyfrowanie, ale nie wysyła pełnego szyfrogramu, tylko najważniejsze 32 bity
 - pozostałe bity są używane do tworzenia kluczy szyfrujących dla sesji



Protokoły - uwierzytelnienie: Bluetooth

- ❑ Klucz łącza dla jednego połączenia jest tworzony podczas procedury zwanej *Bluetooth Pairing*
 - do obliczenia klucza łącza służy klucz inicjalizacyjny
 - Klucz inicjalizacyjny zależy od PINu
- ❑ Należy chronić urządzenia przed podsłuchem podczas *pairing*
- ❑ Należy używać długich PINów - łatwo jest złamać PIN, zmieniając swój adres MAC

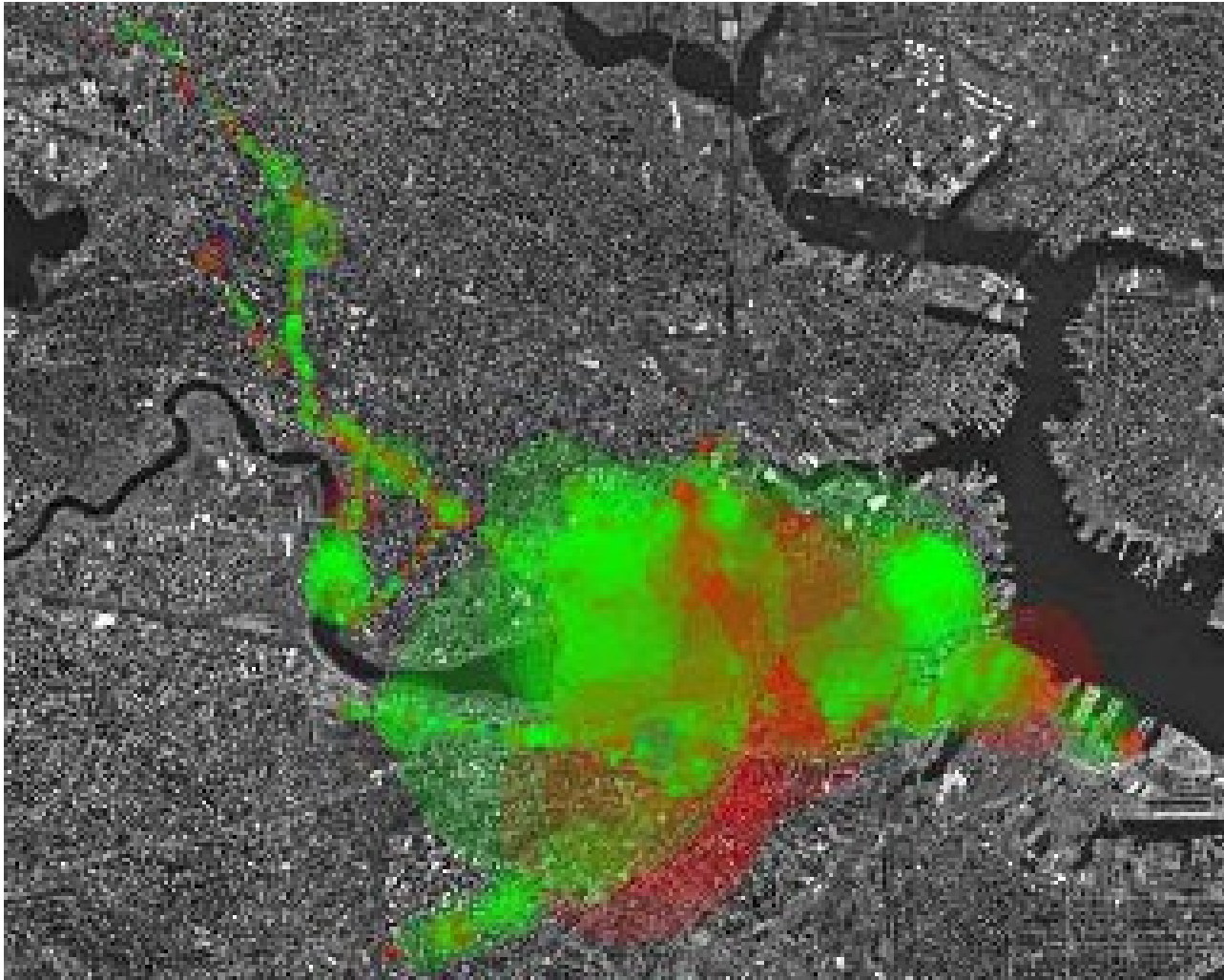
Plan wykładu

- ❑ Wstęp: bezprzewodowe sieci lokalne (WLAN)
- ❑ Proste formy zabezpieczeń
- ❑ Protokoły
 - Poufność
 - WiFi: WEP, WPA, WPA2/802.11i
 - Bluetooth
 - Uwierzytelnienie
 - WiFi: WEP, WPA-PSK, WPA-EAP
 - Bluetooth
- ❑ **Naruszenia bezpieczeństwa sieci**
 - Wardriving, Warflying, Warchalking...
 - Wrogie punkty dostępowe
 - Zagrożenia WiFi, Bluetooth
 - Metody ochrony

Wardriving, Warflying, Warchalking...



Wardriving, Warflying, Warchalking...






Mapka Bostonu – topografia WiFi..

SKO2

Mobilne-103

Wardriving, Warflying, Warchalking...

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid 
WEP NODE	ssid access contact  bandwidth

blackbeltjones.com/warchalking
The original three "warchalk" designs spawned off a larger set of symbols.



Co, jeśli zobaczysz taki znak na swoim domu...?

Zagrozenie totalne

- ❑ Na nic wszystkie zabezpieczenia...
- ❑ ...jeśli napastnik kontroluje punkt dostępowy!
- ❑ Wszelkie metody szyfrowania są bezużyteczne
- ❑ Uwierzytelnienie często jest nieskuteczne: np. bazuje na adresie MAC
- ❑ Nawet jeśli uwierzytelnienie jest skuteczne, trzeba mieć zaufanie do punktu dostępowego

Zagrożenia WiFi

- ❑ Wrogie punkty dostępowe
 - punkty dostępowe o silniejszym sygnale
 - punkty dostępowe zmieniające MAC
 - Evil twin
- ❑ Źle skonfigurowane punkty dostępowe
 - otwieranie drogi do własnej sieci
 - ...a może do sieci firmy? Złośliwie?
- ❑ Połączenie ad-hoc

Zagrożenia Bluetooth

- ❑ Bluetooth ma zasięg...
 - 10m?
 - 100m??
 - 1000m??!!! (z anteną kierunkową)
- ❑ PINy to często jest żart
 - zachowywane są fabryczne ustawienia
- ❑ W takiej sytuacji, klawiatura bądź słuchawka Bluetooth nabiera zupełnie nowych zastosowań...

Jak się chronić?

❑ Planowanie sieci WiFi

- ustawienie punktów dostępowych z dala od fizycznych granic obszaru organizacji
- rejestracja wszystkich punktów dostępowych
- mapa pola radiowego wraz z wizualizacją

❑ Stosowanie systemów IPS

- **Intrusion Prevention Systems**
- Lokalizacja i fizyczna reakcja na pojawienie się napastnika

❑ Unikanie WiFi w instytucjach, dla których bezpieczeństwo informacji ma kluczowe znaczenie