



Sieci komputerowe

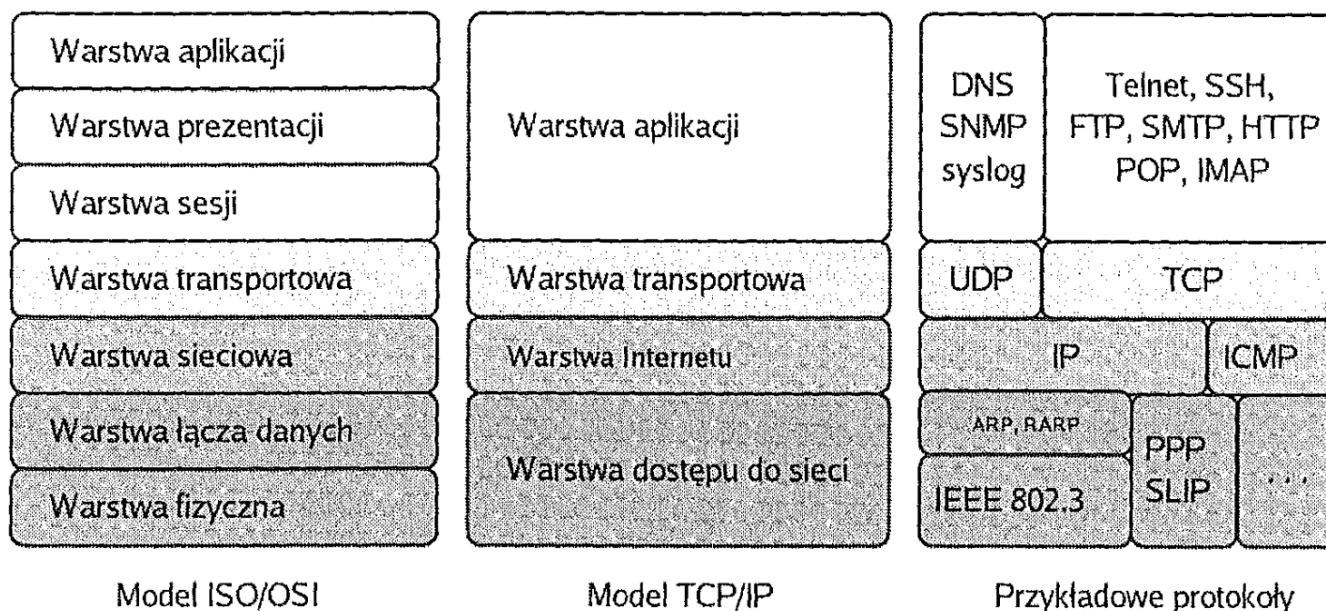
Wykład 2
14.10.2019

dr inż. Łukasz Graczykowski
lukasz.graczykowski@pw.edu.pl

Semestr zimowy 2019/2020

Warstwy modelu ISO

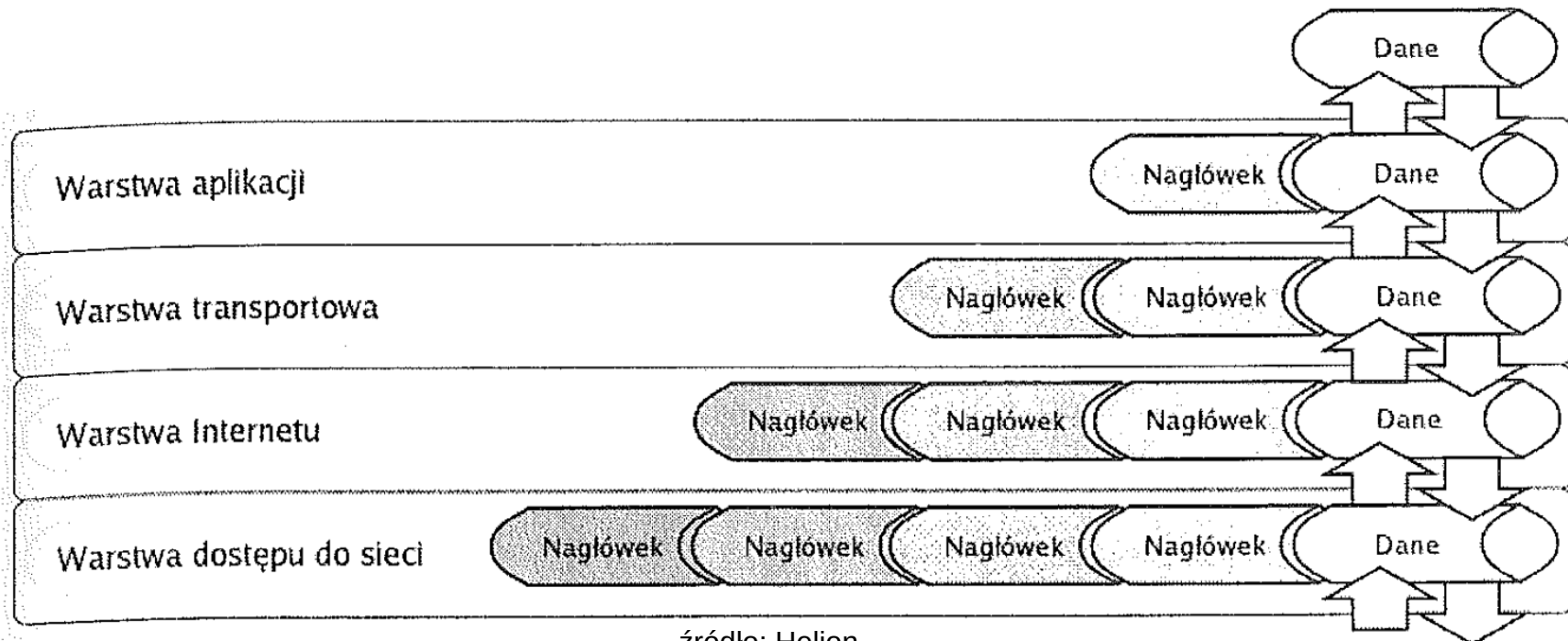
- **Model ISO/OSI** dzieli proces transmisji danych na 7 etapów, zwanych *warstwami*
- Dane przekazywane są zawsze od warstwy najwyższej do najniższej, trafiają do odbiorcy, i następnie zamieniane są na zrozumiałą wiadomość od warstwy najniższej do najwyższej
- **W modelu TCP/IP wyróżniamy 4 warstwy** (poprzez łączenie funkcjonalności pozostałych)



źródło: Helion

Enkapsulacja danych

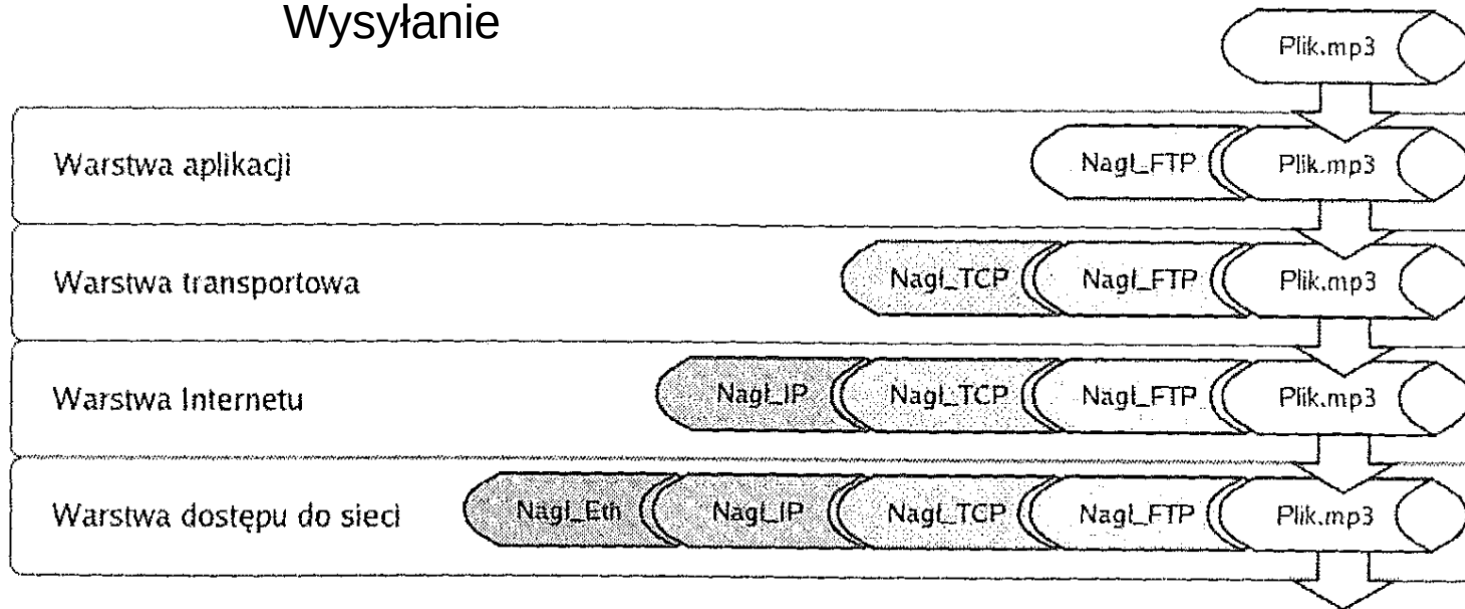
- **Enkapsulacja** danych polega na dołączaniu przez kolejne warstwy swoich nagłówków (np. numer portu czy adres IP)
- W odbiorze, każda warstwa rozpoznaje swój **nagłówek**, usuwa go przekazując dane wyżej, aż do konkretnej aplikacji, która prezentuje dane użytkownikowi



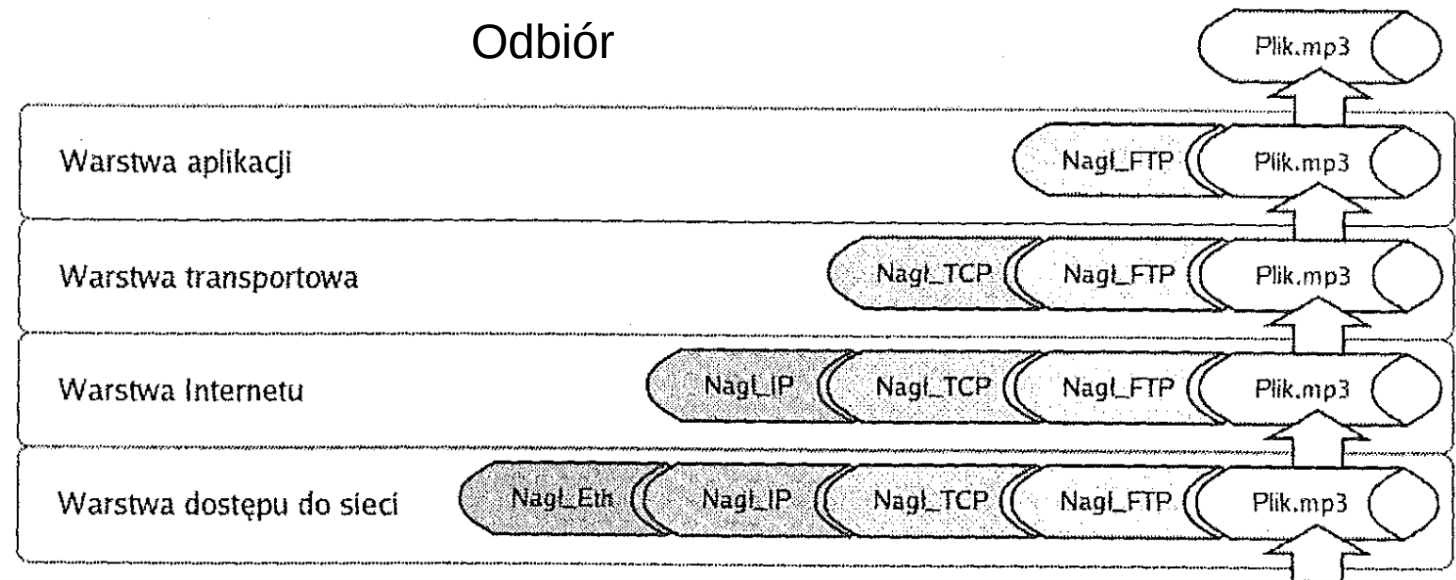
źródło: Helion

Enkapsulacja danych

Wysyłanie



Odbiór



źródło: Helion

Nazewnictwo jednostek danych

- Dane w różnych warstwach posiadają różne nazewnictwo
- Wynika ono z sekwencjonowania danych – nie mamy jednego, potencjalnie nieskończonego ciągu danych, a pewien zbiór segmentów (trochę jak jednostki miar w fizyce)

Tabela 1.1. *Nazwy jednostek danych dla kolejnych warstw modelu TCP/IP*

Warstwa	TCP	UDP
Aplikacji	strumień	wiadomość
Transportowa	segment	pakiet
Internetu		datagram
Dostępu do sieci		ramka

źródło: Helion

- W nomenklaturze CISCO (częściej spotykana) mamy:
 - warstwa Internetu – **pakiet**
 - warstwa dostępu do sieci – **ramka**



Warstwa dostępu do sieci Ethernet

Historia

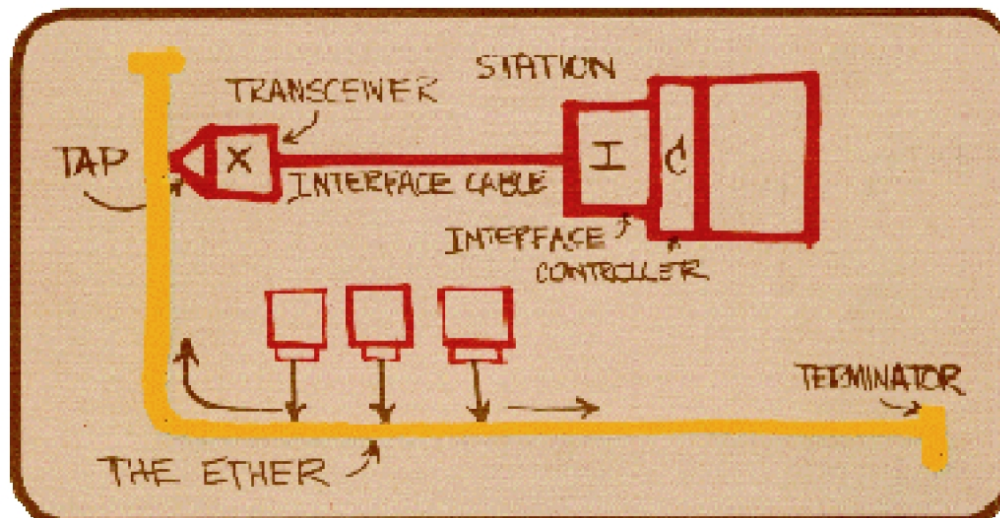
- Opracowana poprzez inspirację ALOHAnet przez Roberta Metcalfe i Davida Boggs z Xerox Palo Alto Research Center
- *Ethernet: Distributed Packet Switching for Local Computer Networks*, Communications of the ACM 19(1):395-404, 1976
- Formalna specyfikacja:
 - konsorcjum Intel, Xerox, DEC (Digital Equipment)
 - 1985 – IEEE ustanowił standard IEEE 802.3 zwyczajowo **Ethernet**

Computer
Systems

G. Bell, S. Fuller and
D. Siewiorek, Editors

Ethernet: Distributed Packet Switching for Local Computer Networks

Robert M. Metcalfe and David R. Boggs
Xerox Palo Alto Research Center



Ethernet is a branching broadcast communication system for carrying digital data packets among locally distributed computing stations. The packet transport

Notatka Roberta Metcalfe

Historia

XEROX

ETHER!



MEMO

MAY 22, 1973

TO: ALTO ALOHA DISTRIBUTION
FROM: BOB METCALFE
SUBJECT: ETHER ACQUISITION

HERE IS MORE ROUGH STUFF ON THE ALTO ALOHA NETWORK.

I PROPOSE WE STOP CALLING THIS THING "THE ALTO ALOHA NETWORK". FIRST, BECAUSE IT SHOULD SUPPORT ANY NUMBER OF DIFFERENT KINDS OF STATION -- SAY, NOVA, PDP-11, SECOND, BECAUSE THE ORGANIZATION IS BEGINNING TO LOOK VERY MUCH MORE BEAUTIFUL THAN THE ALOHA RADIO NETWORK -- TO USE CHARLES'S "BEAUTIFUL".

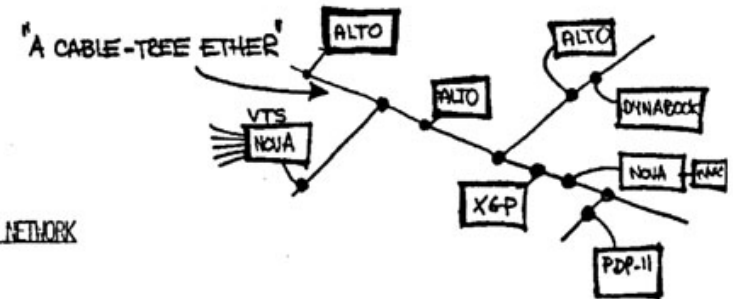
MAYBE: "THE ETHER NETWORK". SUGGESTIONS?

LAZY SUZAN
BULLETIN BOARD
PARLEY
PARLIAMENTARY
PROCEDURE

I HOPE TO BE SIMULATING SOON. HELP? INPUTS?

I HOPE YOU WILL NOT BE OFFENDED BY MY ATTEMPTS TO MAKE THIS THINKING AND DESIGN APPEAR THEORETICAL.

XEROX

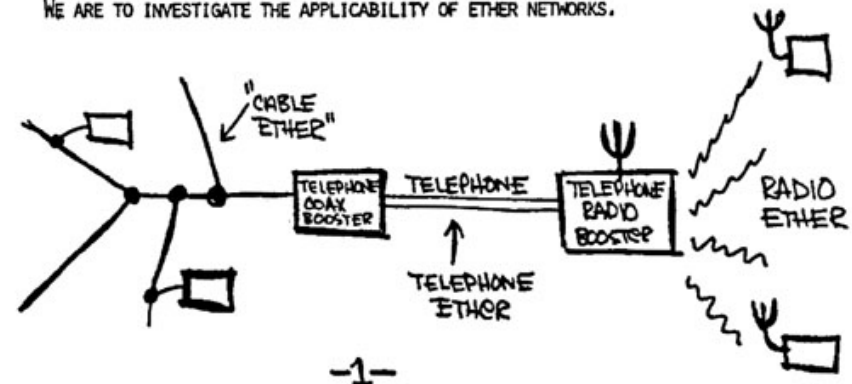


THE ETHER NETWORK

WE PLAN TO BUILD A SO-CALLED BROADCAST COMPUTER COMMUNICATION NETWORK, NOT UNLIKE THE ALOHA SYSTEM'S RADIO NETWORK, BUT SPECIFICALLY FOR IN-BUILDING MINICOMPUTER COMMUNICATION. WE THINK IN TERMS OF NOVA'S AND ALTO'S JOINED BY COAXIAL CABLES.

WHILE WE MAY END UP USING COAXIAL CABLE TREES TO CARRY OUR BROADCAST TRANSMISSIONS, IT SEEMS WISE TO TALK IN TERMS OF AN ETHER, RATHER THAN 'THE CABLE', FOR AS LONG AS POSSIBLE. THIS WILL KEEP THINGS GENERAL AND WHO KNOWS WHAT OTHER MEDIA WILL PROVE BETTER THAN CABLE FOR A BROADCAST NETWORK; MAYBE RADIO OR TELEPHONE CIRCUITS, OR POWER WIRING OR FREQUENCY-MULTI-PLEXED CATV, OR MICROWAVE ENVIRONMENTS, OR EVEN COMBINATIONS THEREOF.

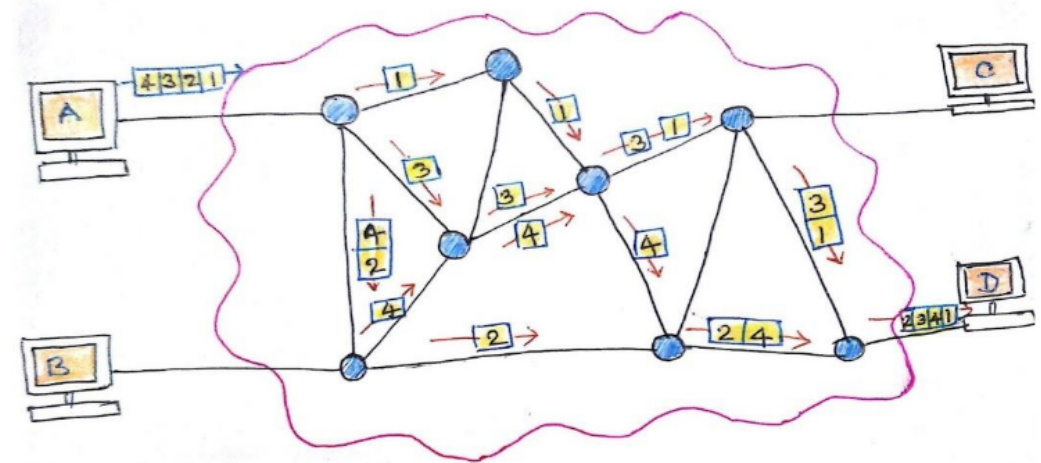
THE ESSENTIAL FEATURE OF OUR MEDIUM -- THE ETHER -- IS THAT IT CARRIES TRANSMISSIONS, PROPAGATES BITS TO ALL STATIONS. WE ARE TO INVESTIGATE THE APPLICABILITY OF ETHER NETWORKS.



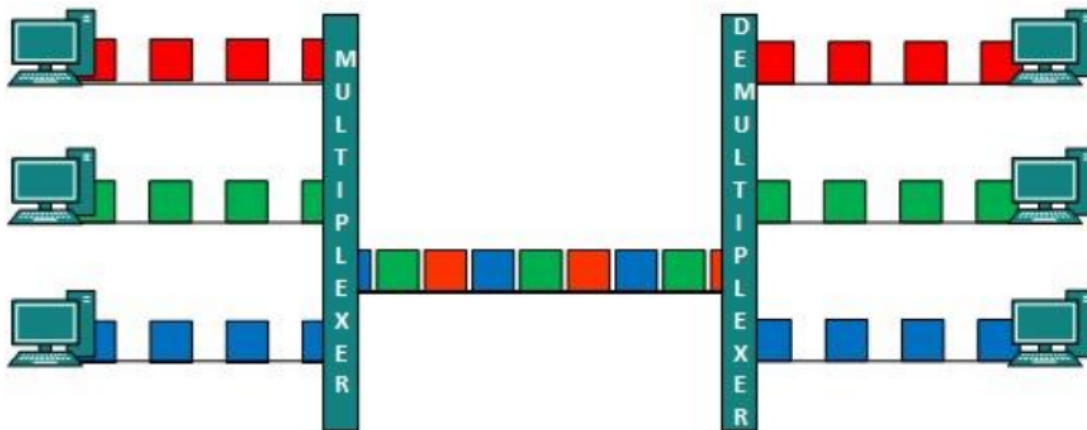
Działanie Ethernetu

- Sieci komputerowe w standardzie ethernet wykorzystują **komutację pakietów**:

- transfer informacji przez węzły
- podział informacji na części o stałej długości (pakiety)
- współdzielenie łącza
- nagłówki i sprawdzanie poprawności danych



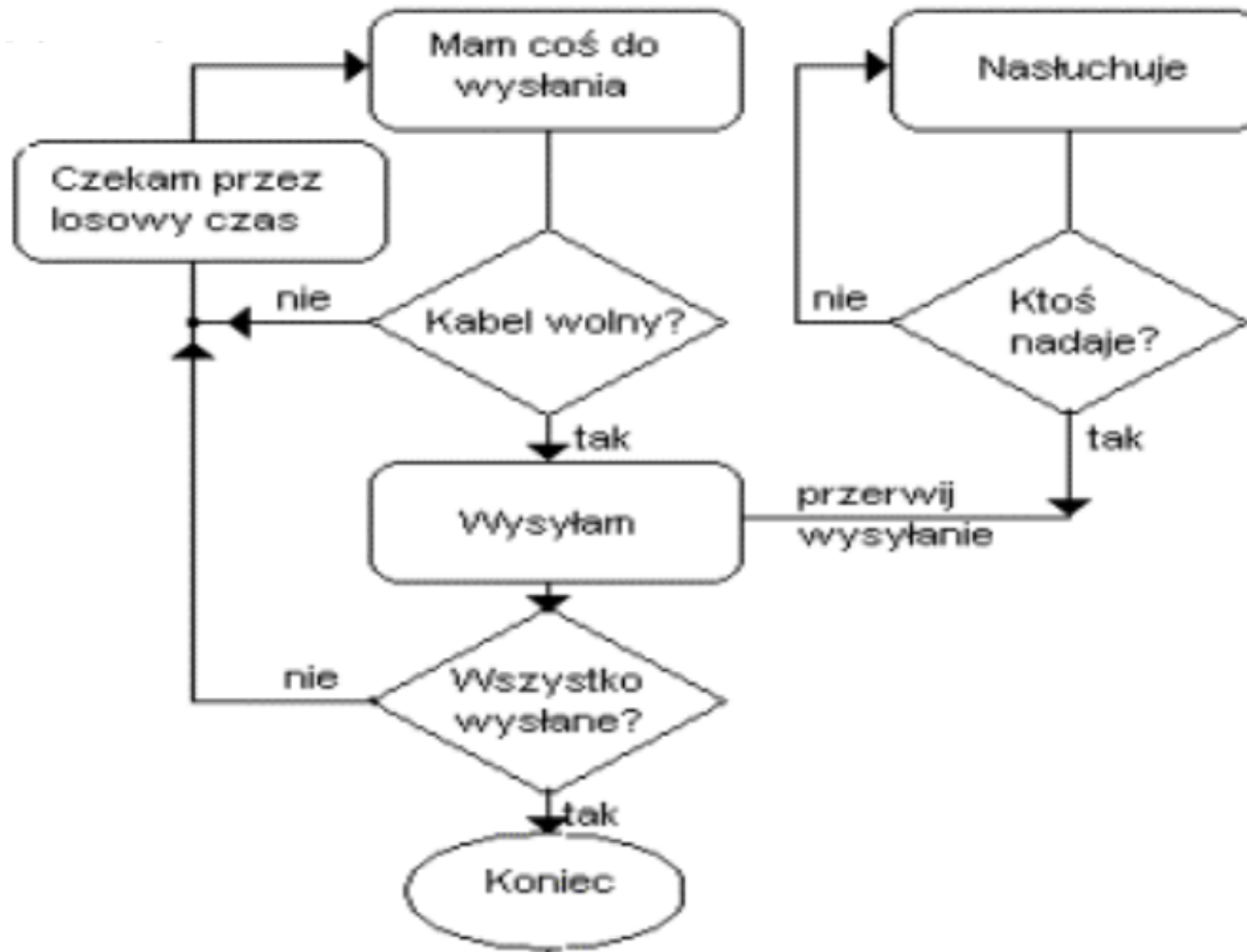
Datagram approach



Działanie Ethernetu

- Wyróżniamy trzy metody transmisji danych (w kolejności historycznej)
 - ALOHA – nadajemy w dowolnym momencie i czekamy na potwierdzenie odbioru, jeśli nie nadchodzi to ponawiamy → problem **kolizji** (sieć się zapycha, dane się zniekształcają)
 - CSMA (Carrier Sense, Multiple Access) – ciągły nasłuch łącza, gdy łącze wolne rozpoczynamy nadawanie, kolizja możliwa jedynie wtedy, gdy dwie stacje rozpoczną nadawanie w tym samym czasie, oczywiście dowiedzą się o tym i powtórzą transmisję...
 - CSMA/CD (with Collision Detection) – po wykryciu kolizji powtarza sygnał, ale nie przerywa od razu, zniekształcony sygnał jest nadal wysyłany, aby zwiększyć prawdopodobieństwo wykrycia kolizji przez innych (dopiero po chwili jest wysyłany ponownie)

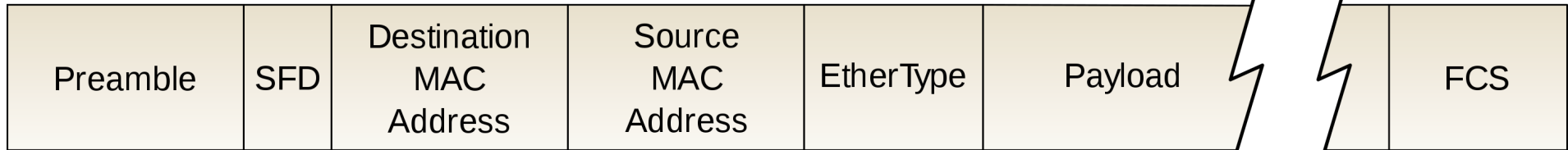
CSMA/CD



Noma IEEE 802.3

- Przesyłanie informacji następuje w ramach ethernetowych (patrz enkapsulacja danych) – ramka jest jednostką danych

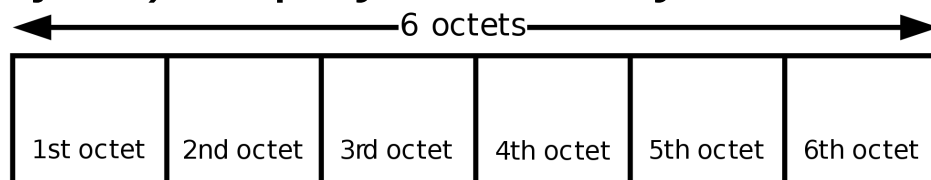
źródło: Wikipedia.org



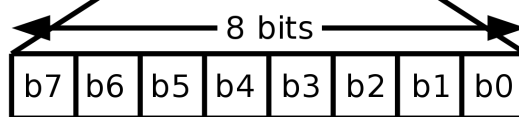
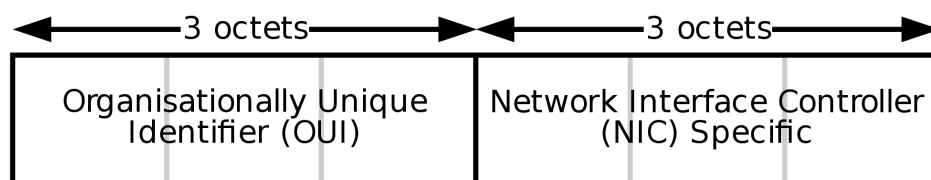
- Preambuła** – naprzemienny ciąg bitów 0 i 1 informujący o nadchodzącej ramce, 7 bajtów
 - SFD** – bajt kończący preambułę (zawsze zakończony dwoma bitami 11)
 - Adresy** (*MAC – Media Access Control*) – 6-bajtowe liczby będące adresami sprzętowymi komunikujących się urządzeń, przyznawane przez IEEE, nie powinno być 2 kart sieciowych o tym samym adresie
 - EtherType** (2 bajty) – używany do określenia długości pola danych
 - Payload** – przesyłana informacja (nasze dane)
 - FCS** – 4 bajty kontrolne (*CRC – Cyclic Redundancy Check*), generowane przez interfejs nadający i sprawdzane przez odbierający
- Cała ramka** – od 64 do 1518 bajtów

Adres MAC

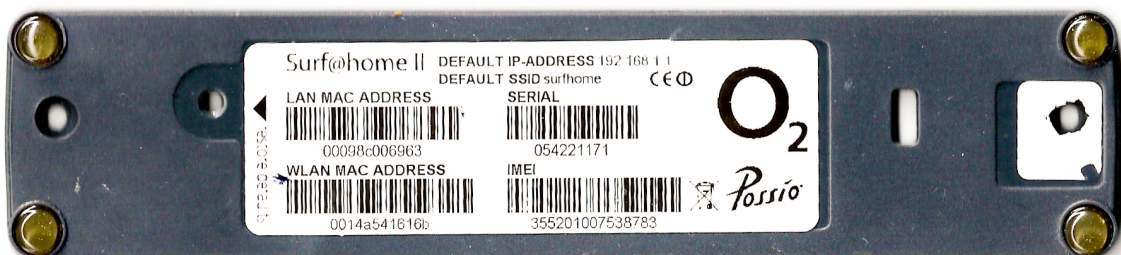
- Adresacja w warstwie łącza danych, funkcjonująca zarówno w Ethernetie jak i np. WiFi
 - **adres MAC** jest unikalny w skali światowej (przyznawane przez IEEE i ostatecznie ustalane przez producenta urządzenia)
 - adres zawsze ma 48 bitów (6 bajtów), zapisywane w systemie heksadecymalnym
 - przykładowy adres MAC:
B5:AD:C3:2A:D4:F1
 - **adres IP jest ustalany na wyższych warstwach**
→ **fizycznie wysyłamy na MAC**



or



źródło: Wikipedia.org

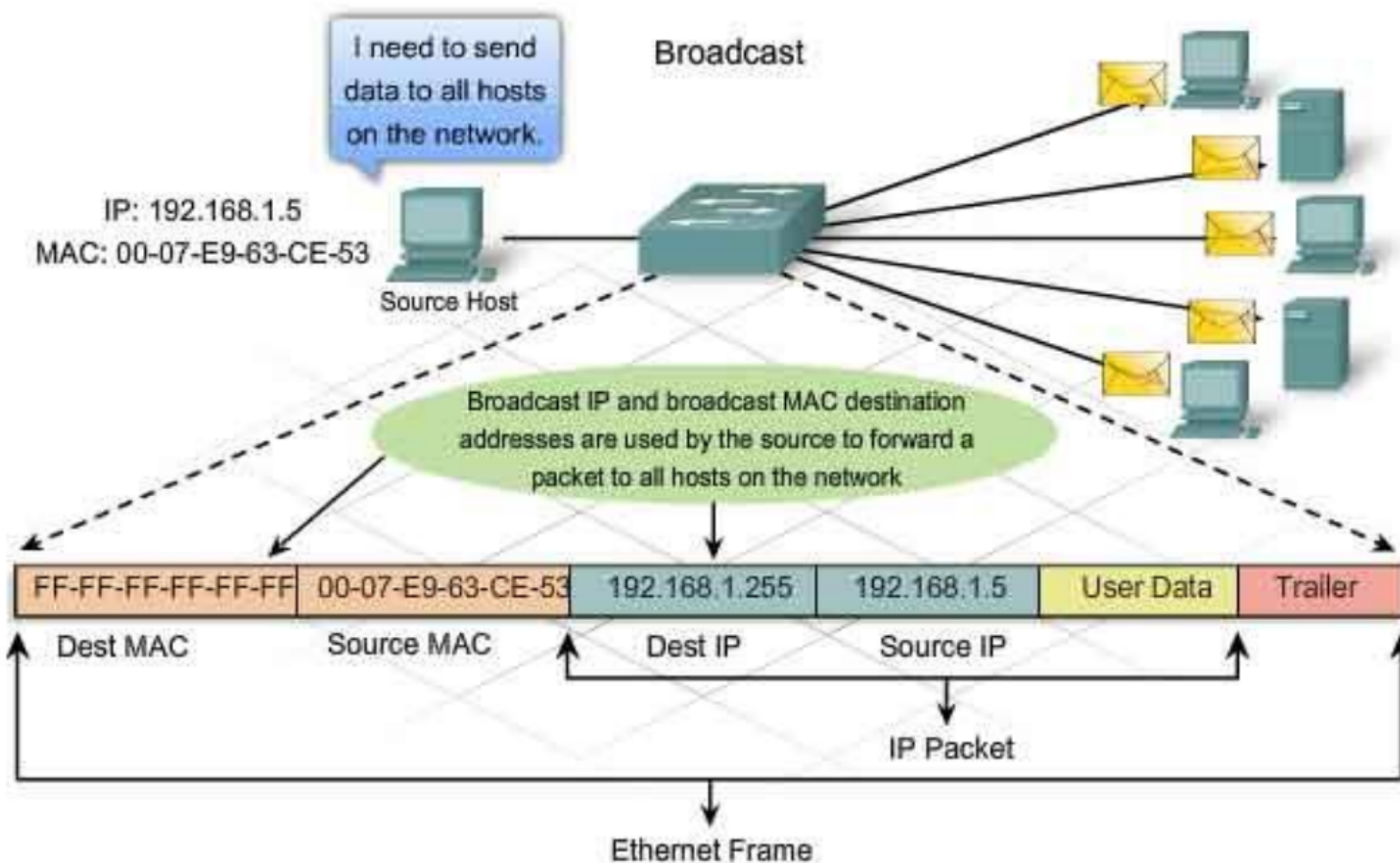


0: unicast
1: multicast

0: globally unique (OUI enforced)
1: locally administered

Adres MAC

- Wyróżniamy również adresy specjalne (zarówno MAC jak i IP):
 - **multicast** – odbieranie ramki przez grupę stacji (01:00:5E:XX:XX:XX)
 - **broadcast** – odbieranie ramki przez wszystkie stacje (FF:FF:FF:FF:FF:FF)



Noma IEEE 802.3

- Standard ethernet IEEE 802.3 opisany jest przez metodę CSMA/CD
- Norma IEEE 802.3 definiuje parametry techniczne łącz o odpowiednich prędkościach, przykładowo:

Tabela 3.1. Dane techniczne dla szybkości 10 Mb/s (standard IEEE 802.3)

Odstęp międzyramkowy — IFG	9,6 μ s
Ilość bitów wyznaczających szczelinę czasową	512 b
Szerokość szczeliny czasowej	51,2 μ s
Czas wymuszania kolizji	3,2 μ s
Maksymalna długość ramki	1518 B
Minimalna długość ramki	64 B
Maksymalna rozpiętość sieci	2000 m

- Aby działać w danej prędkości, wszystkie urządzenia w sieci muszą spełniać wymagania danego standardu:
 - przykładowo 100Base-T – parametry skrętki 100 Mb/s
 - **podpięcie kabla o wyższych parametrach do urządzenia o niższych nie spowoduje, że sieć będzie działała szybciej!**

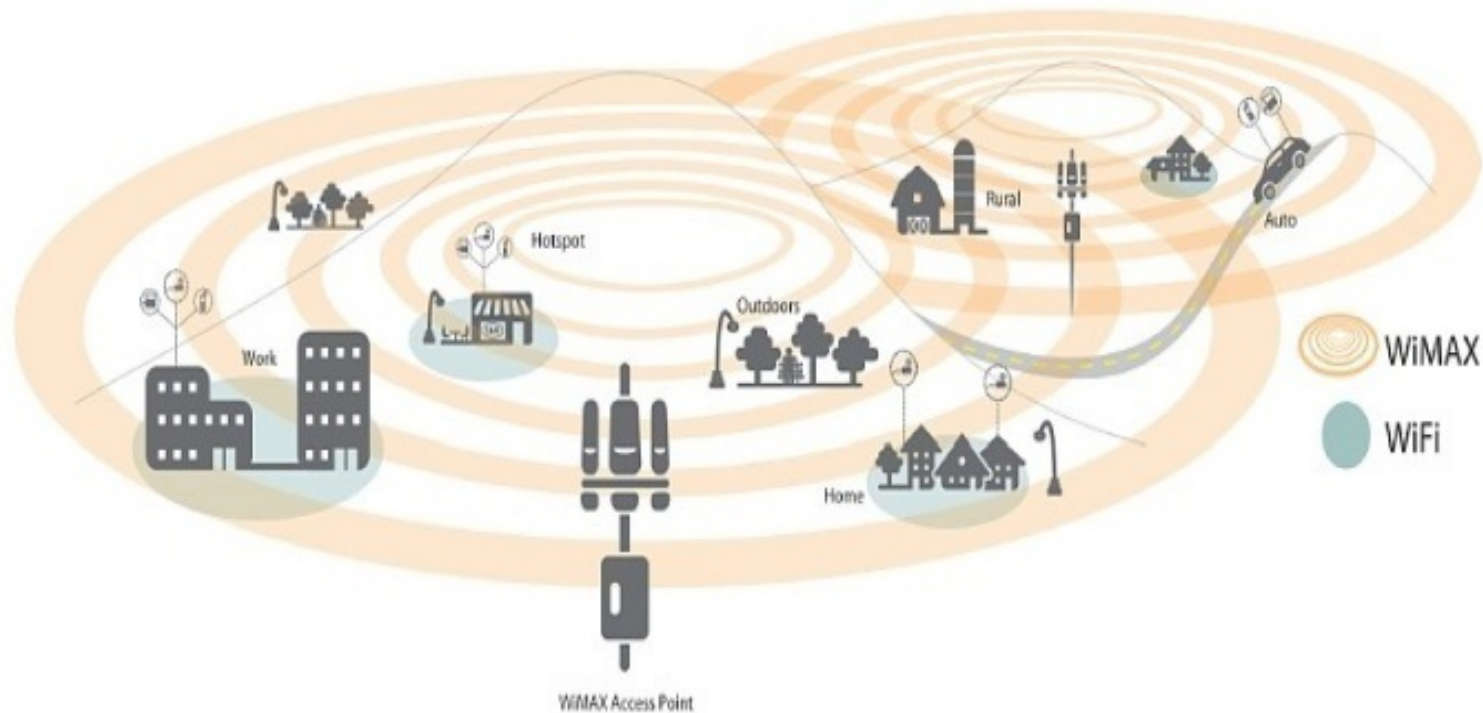
WiFi – standard IEEE 802.11

- **WLAN** (Wireless LAN) – standard IEEE 802.11
- Wi-Fi Alliance jest organizacją non-profit, która certyfikuje urządzenia i zapewnia ich interoperacyjność
 - **nie każde urządzenie zgodne z 802.11 musi być certyfikowane przez Wi-Fi!**
- Pierwsza wersja powstała w 1997 roku i pozwalała na transmisję danych 1 lub 2 Mb/s w podczerwieni lub za pomocą fal radiowych 2.47 GHz → w zasadzie niespotykana
- 802.11b – transfer danych do 11 Mb/s (w rzeczywistości nieosiągalny) i pełna zgodność z 802.11
- Kolejno nowsze standardy (generacje) 802.11g, 802.11n, itp.
- Zwykle nowe urządzenia operują również na częstotliwości 5 GHz



WiFi – standard IEEE 802.11

- Istnieją też inne standardy, np. WiMAX (IEEE 802.16)



WiFi – standard IEEE 802.11

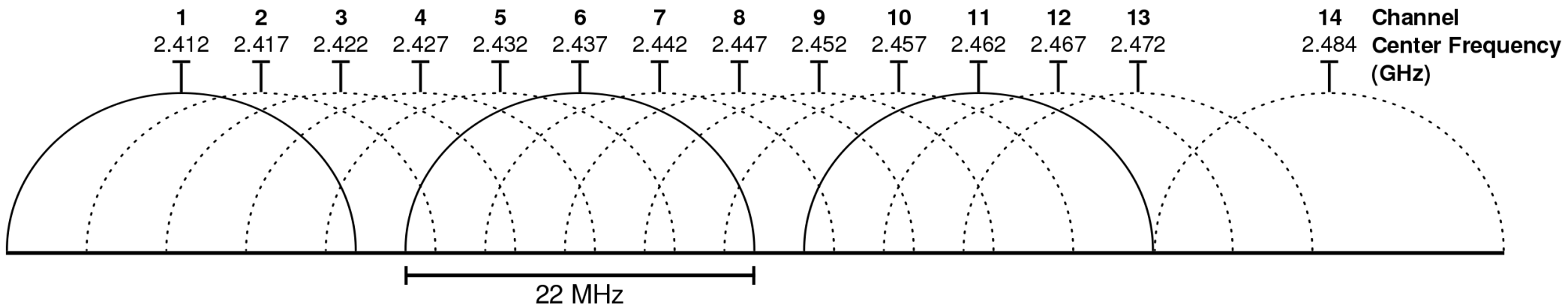
Tabela 4.1. Porównanie standardów transmisji bezprzewodowej

	Standard					
	IrDA	Bluetooth	IEEE 802.11	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g
Zasięg	1 m	10 m	60 m	100 m	75 m	100 m
Maksymalna szybkość transmisji	4 Mb/s	1 Mb/s	2 Mb/s	11 Mb/s	54 Mb/s	54 Mb/s
Medium	podczerwień	fale radiowe				
Wrażliwość na zakłócenia	duża	średnia	średnia	mała	średnia	duża
Długość fali/ częstotliwość	850 – 900 nm	2,4 GHz	2,4 GHz	2,4 GHz	5 GHz	2,4 GHz
Data zatwierdzenia	1993 r.	1998 r.	06.1997 r.	08.1999 r.	08.1999 r.	06.2003 r.

źródło: Helion

WiFi – standard IEEE 802.11

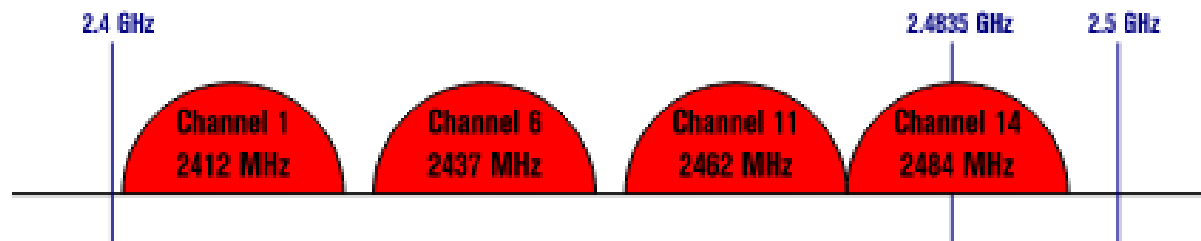
- Dostępne pasmo dzieli się na **kanały**
- W standardach typu 802.11g **14 kanałów**:
 - pasma oddalone od siebie o 5 MHz
 - pasma się na siebie **nakładają**



- bez zakłóceń wybieramy kanały **1, 6 i 11**

Non-Overlapping Channels for 2.4 GHz WLAN

802.11b (DSSS) channel width 22 MHz



WiFi – standard IEEE 802.11

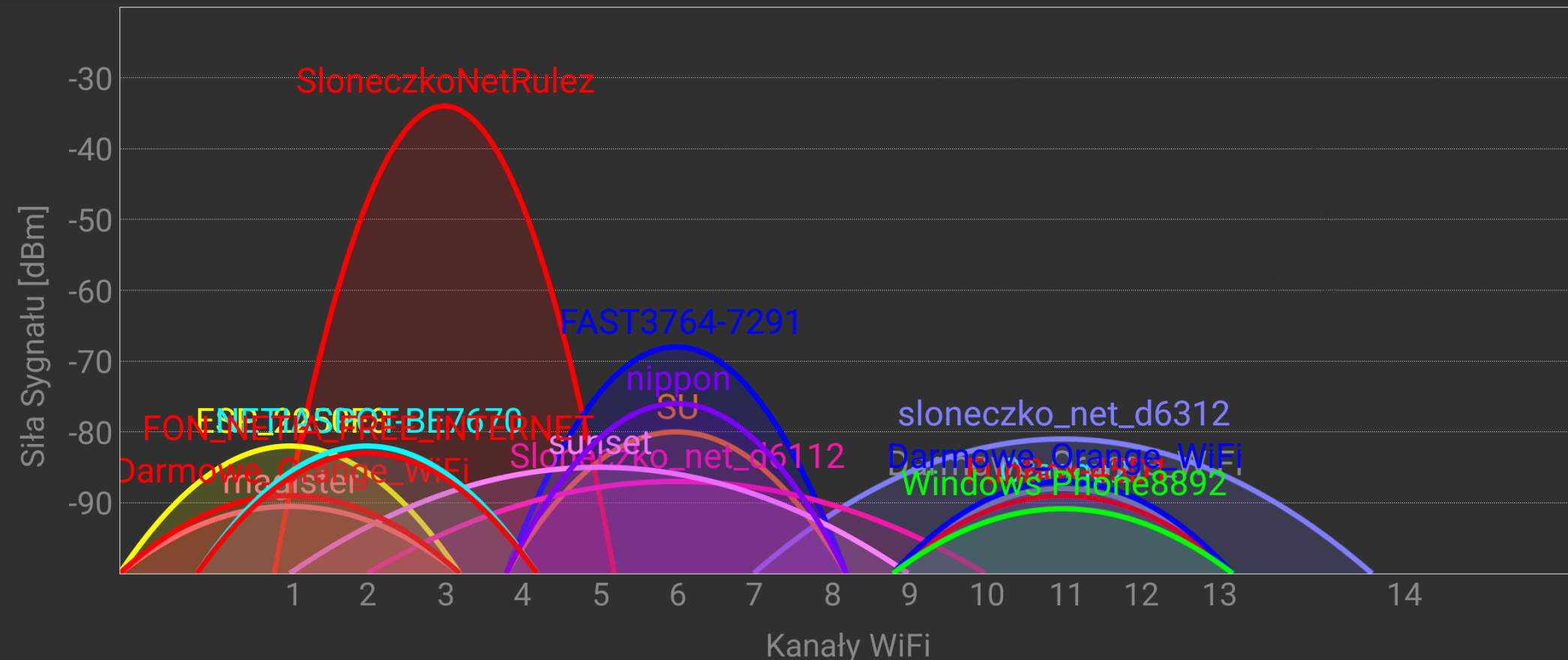
- W praktyce zwykły użytkownik tego nie sprawdza i potem to wygląda tak...



Wifi Analyzer

ZOBACZ

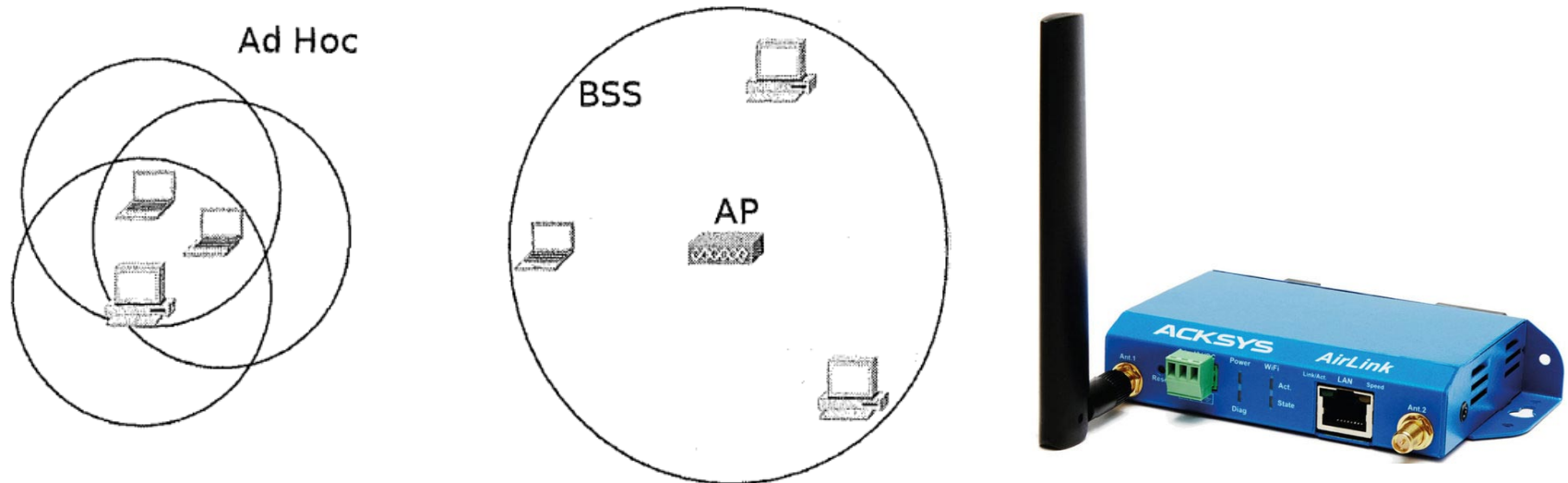
USTAWIENIA



WiFi – struktura sieci WLAN

- Proste sieci WLAN możemy tworzyć jako:
 - **ad hoc** (*IBSS*) – komputery łączą się za pomocą swoich kart sieciowych
 - **BSS** (*Basic Service Set*) – używając punktu dostępowego (*access point* – **AP** – odpowiednik koncentratora w ethernecie)

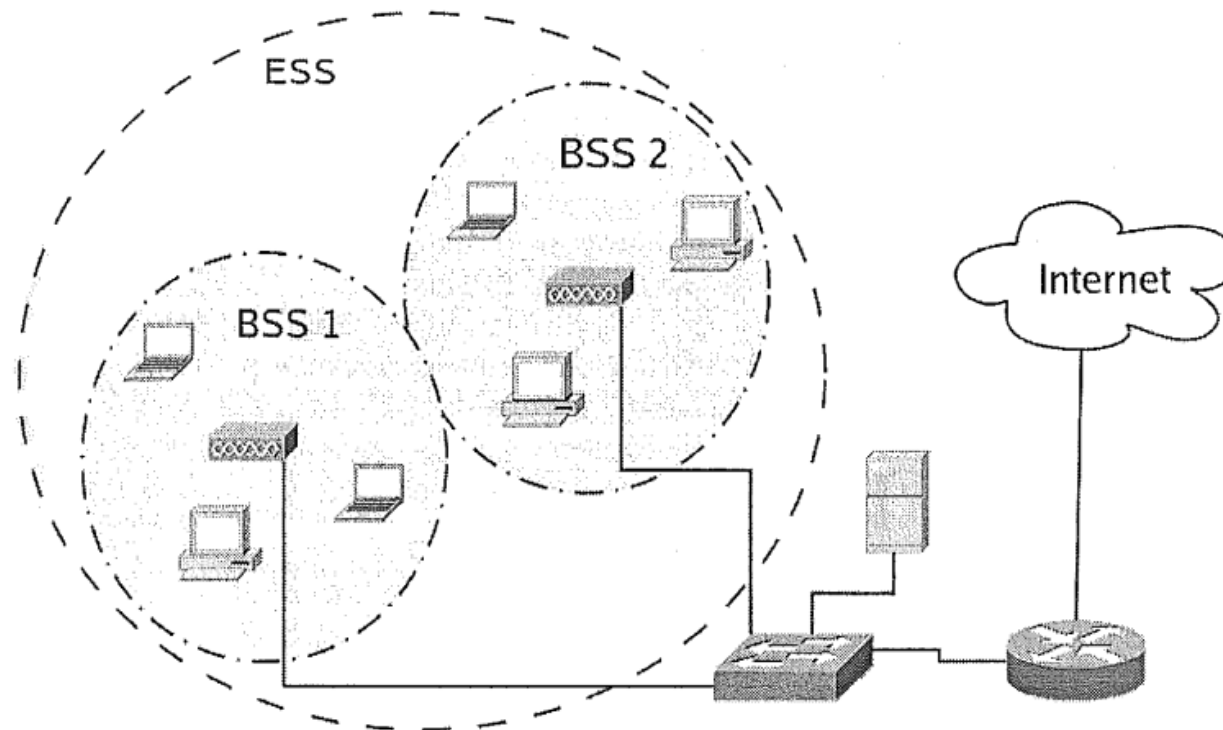
Rysunek 4.2.
Sieć Ad Hoc i BSS



- Najczęściej sieć WLAN jest uzupełnieniem sieci LAN opartej na ethernecie i AP jest podłączony kablem ethernetowym z tą siecią

WiFi – struktura sieci WLAN

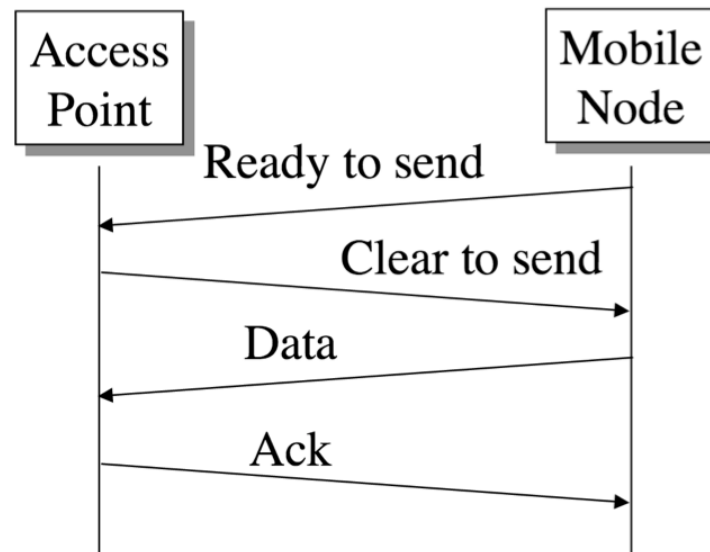
- Jeżeli użyjemy kilka AP (stworzymy kilka BSS) możemy pokryć większy obszar – tworzymy wtedy **ESS** (*Extended Service Set*)
- Jeśli obszary BSS w ESS się przekrywają, mamy do czynienia z **roamingiem** – możemy się przemieszczać między obszarami bez utraty połączenia



Rysunek 4.3. Struktura sieci WLAN

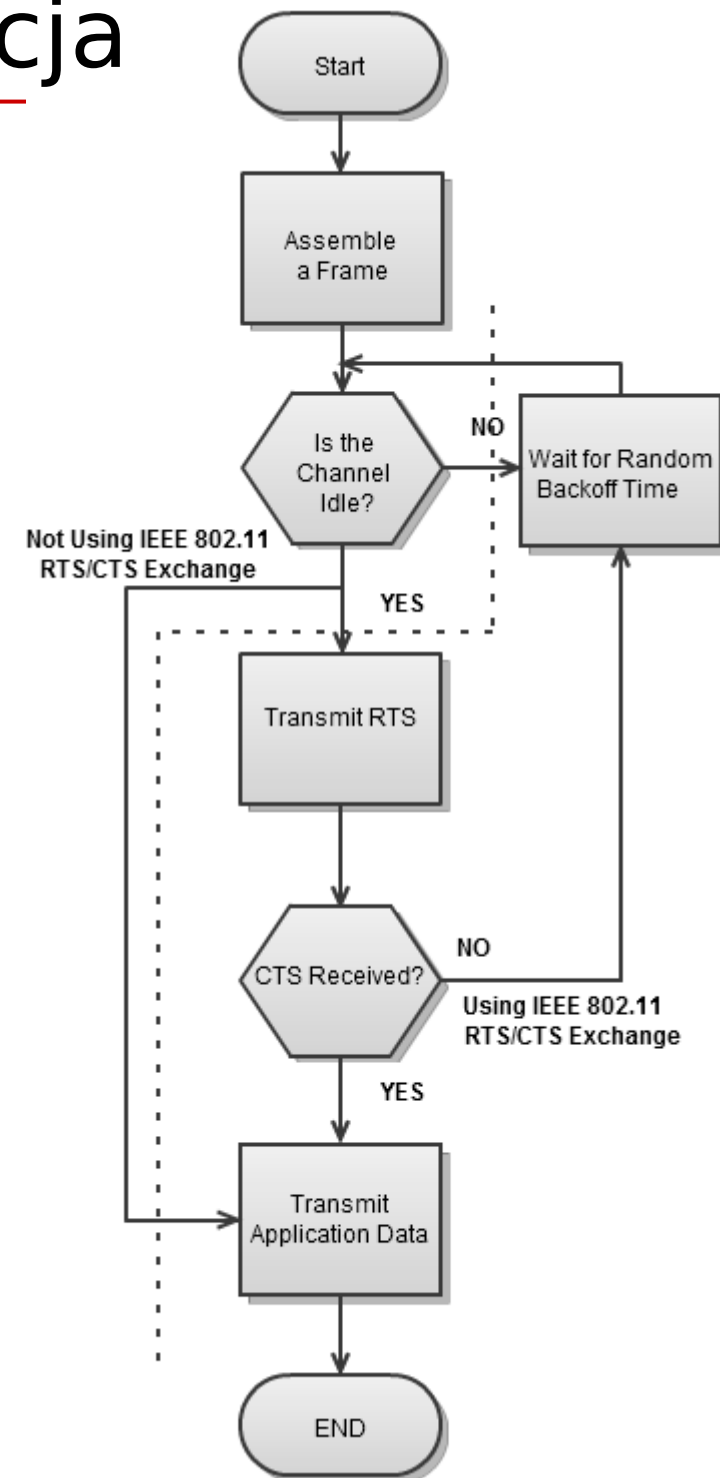
WiFi – komunikacja

- W sieciach WLAN, tak samo jak LAN, możemy mieć do czynienia z problemem kolizji
- W sieciach WLAN nie można stosować CSMA/CD, gdzie jest ciągły nasłuch łącza (zagłuszanie sygnału)
- Stosowany jest system **CSMA/CA** (*with Collision Avoidance*) z dodatkową funkcjonalnością o nazwie **DCF** (*Distributed Coordination Function*)
- Jak to działa? Spójrzmy na algorytm (**4-way handshake**)



WiFi – komunikacja

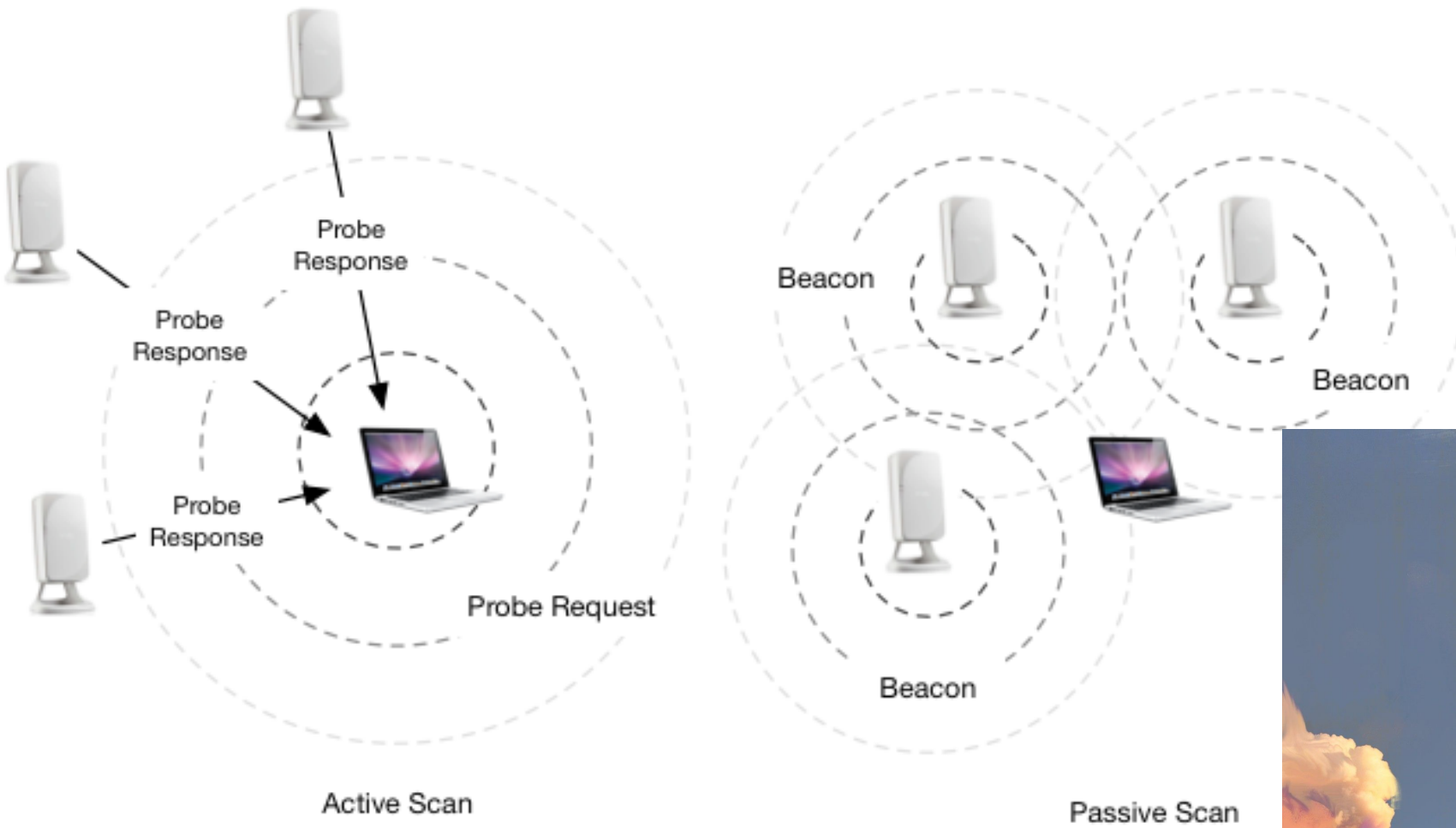
- Nadawca wysyła ramkę **RTS** (*Request To Send*) – informacja o dla innych stacji o zamiarze nadawania
- Odbiorca (np. AP) wysyła ramkę **CTS** (*Clear To Send*) – informacja o gotowości do odbioru
- Po wymianie RTS i CTS, nadawca wysyła właściwą ramkę (inna niż ethernet)
- Odbiorca potwierdza otrzymanie ramki przesłaniem ramki **ACK** (*Acknowledge*)
- Jeśli nadawca nie dostanie ACK, ponawia przesył danych



WiFi – skanowanie

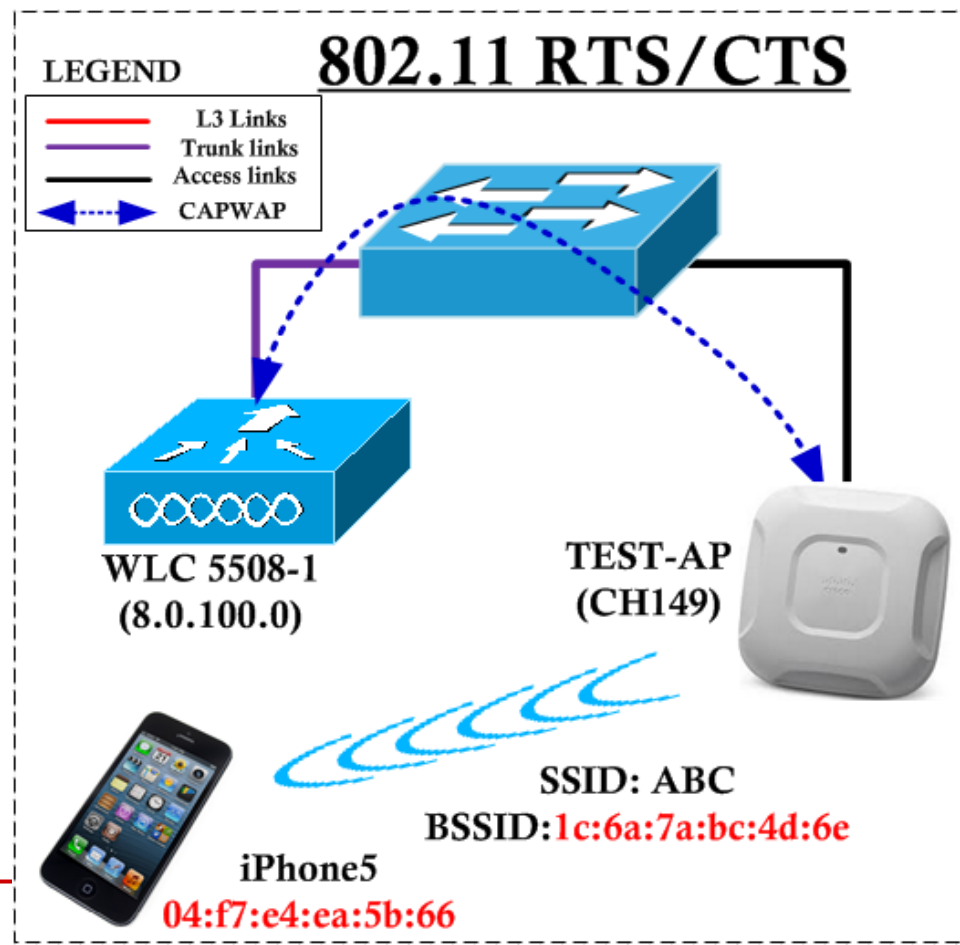
- Stacja bezprzewodowa (np. karta WLAN) może znajdować się w jednym z trzech stanów:
 - **początkowy** – nieuwierzytelniony i nieskojarzony z żadnym punktem dostępowym
 - **uwierzytelniony**
 - **uwierzytelniony i skojarzony** (powiązany) z punktem dostępowym
- Aby połączyć się z siecią, musimy wykonać **skanowanie**:
 - szukamy rozsyłanych co jakiś czas sygnałów **Beacon**, które zawierają informację o danej sieci
 - na bazie siły sygnału **Beacon** wybieramy odpowiedni AP
- **Skonowanie pasywne** – wysłanie **Association Request**
- W **skanowaniu aktywnym** stacja wysyła sygnał próbny **Probe Request**

WiFi - skanowanie



WiFi – parametry sieci

- Niektóre parametry sieci:
 - BSS type – typ sieci (IBSS lub BSS)
 - BSSID – identyfikator danej BSS (MAC adres danego AP)
 - **SSID** (lub ESSID) – nazwa sieci przypisana danym ESS, czyli to co z reguły wybieramy sprawdzając sieci



WiFi - parametry sieci

ESS o dwóch AP



```
PS C:\> netsh wlan show networks mode=bssid

Interface name : Wi-Fi
There are 7 networks currently visible.

SSID 1 : My Movies 5G
Network type      : Infrastructure
Authentication    : WPA2-Personal
Encryption        : CCMP
BSSID 1          : bc:ae:c5:eb:59:8c
Signal           : 88%
Radio type       : 802.11n
Channel          : 36
Basic rates (Mbps) : 6 12 24
Other rates (Mbps) : 9 18 36 48 54

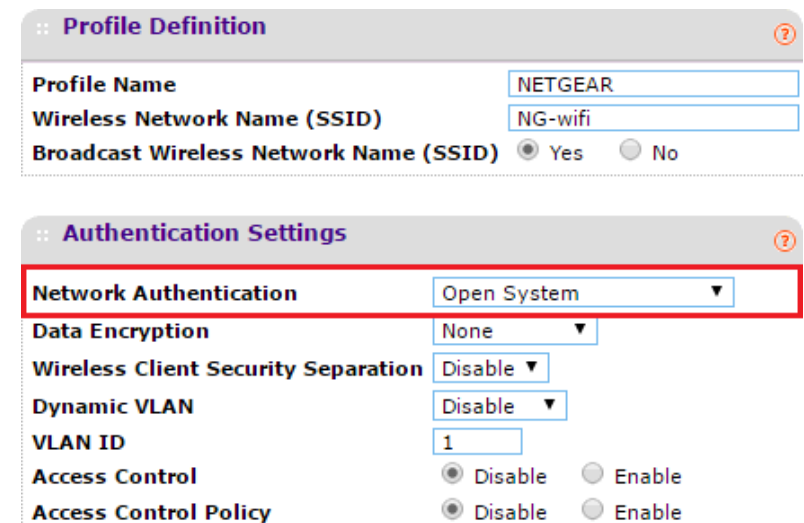
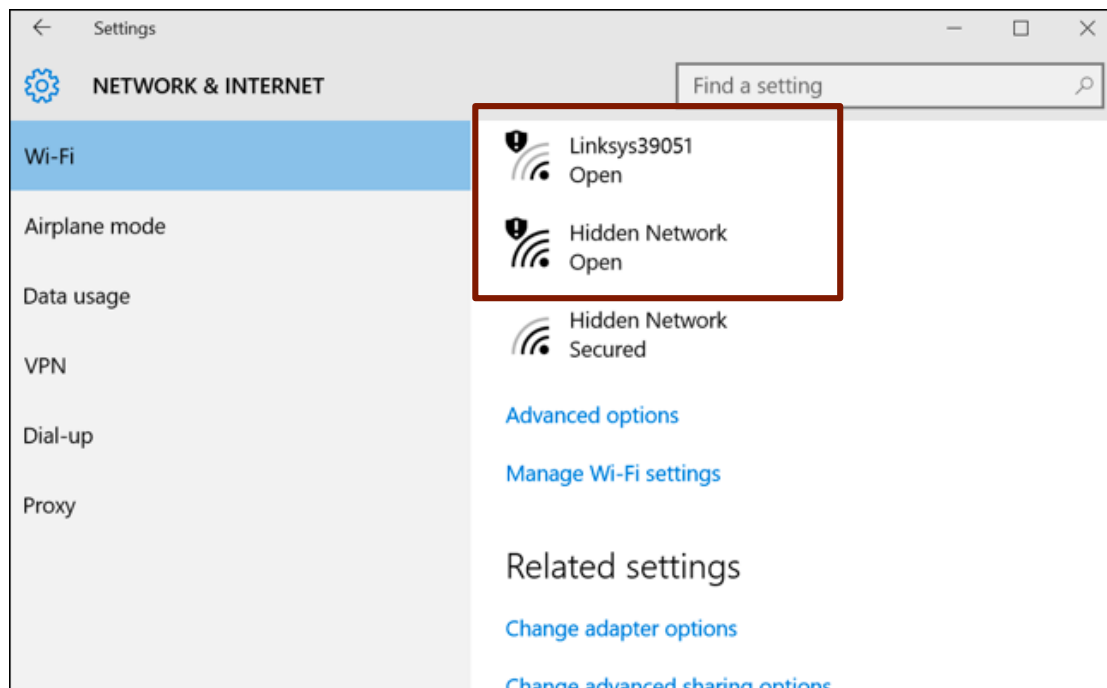
SSID 2 : blackbox
Network type      : Infrastructure
Authentication    : WPA2-Personal
Encryption        : CCMP
BSSID 1          : c8:be:19:aa:98:a4
Signal           : 38%
Radio type       : 802.11n
Channel          : 5
Basic rates (Mbps) : 1 2 5.5 11
Other rates (Mbps) : 6 9 12 18 24 36 48 54

SSID 3 : redbox
Network type      : Infrastructure
Authentication    : WPA2-Personal
Encryption        : CCMP
BSSID 1          : 20:e5:2a:52:d1:38
Signal           : 18%
Radio type       : 802.11n
Channel          : 2
Basic rates (Mbps) : 1 2 5.5 11
Other rates (Mbps) : 6 9 12 18 24 36 48 54

SSID 4 : Greenbox
Network type      : Infrastructure
Authentication    : WPA2-Personal
Encryption        : CCMP
BSSID 1          : 20:c9:d0:28:fb:05
Signal           : 53%
Radio type       : 802.11n
Channel          : 11
Basic rates (Mbps) : 1 2 5.5 11
Other rates (Mbps) : 6 9 12 18 24 36 48 54
BSSID 2          : 20:c9:d0:28:fb:06
Signal           : 45%
Radio type       : 802.11n
Channel          : 100
```

WiFi – połączenie i uwierzytelnianie

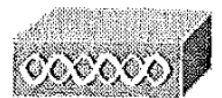
- Połączenie jest dokonywane poprzez wysłanie parametrów stacji do AP
- W standardzie 802.11 zakładamy wiarygodność AP (wada → można stworzyć fałszywy AP) i uwierzytelnianie samego AP spada na stację
- Uwierzytelnianie może być typu **open-system (OSA – Open System Access)** lub **shared-key**



WiFi – połączenie i uwierzytelnianie

- W **shared-key** przy odpowiedzi AP zostaje dołączone do ramki pole **Challenge Text**, np. ma 128 losowych bajtów. W trzecim kroku stacja odsyła zaszyfrowane pole *Challenge Text* (np. WEP) i jeżeli AP odszyfruje tekst i zgadza się on z wysłanym wcześniej, to akceptuje stację
- Po uwierzytelnieniu stacja wysyła **AR** (*Association Request*) i dostaje od AP **AID** (*Association ID*) → kojarzenie (powiązanie)

Rysunek 4.10.
Uwierzytelnianie typu
shared-key



Communication Process

Client

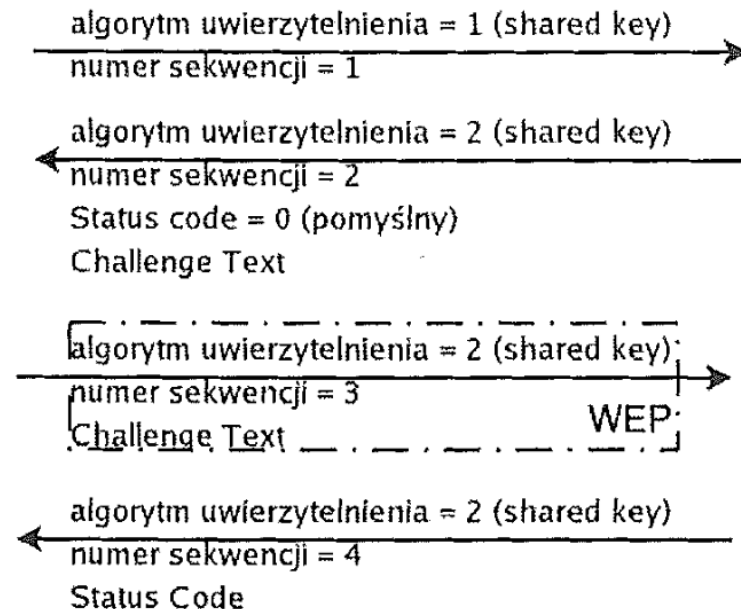


A request to authenticate is sent to the access point

The access point authenticates

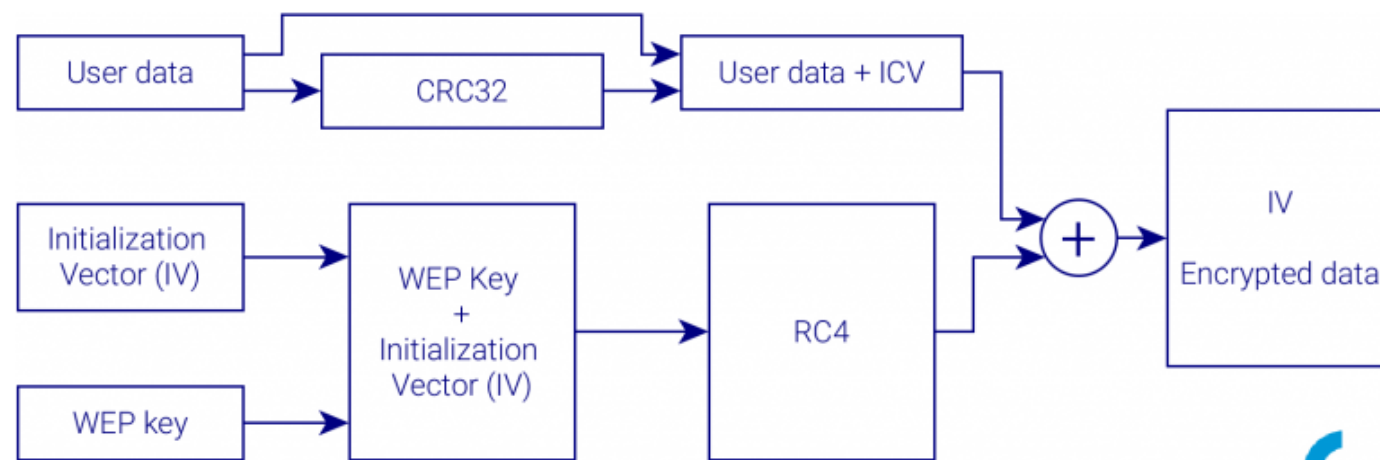
The client connects to the network

Access Point



WiFi – szyfrowanie

- Historycznie używany był protokół **WEP** (*Wired Equivalency Privacy*)
- Do ramki 802.11 jest dodawane odpowiednie pole z kluczem szyfrującym
- Jest zupełnie nieodporny na ataki – łatwo złamać poprzez podsłuchanie 1-2 milionów ramek (darmowe narzędzia)
- Użycie protokołu powoduje zwiększenie długości ramki (mniejsza wydajność)

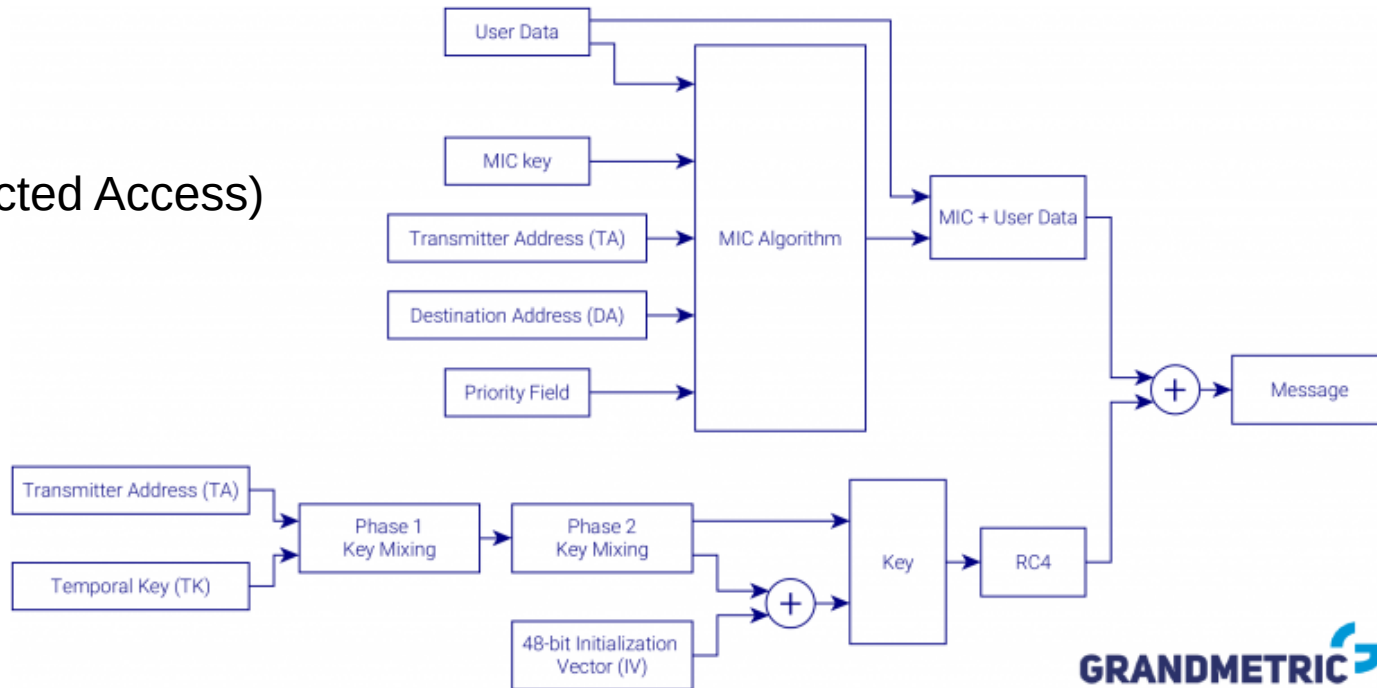


Problemy z WEP

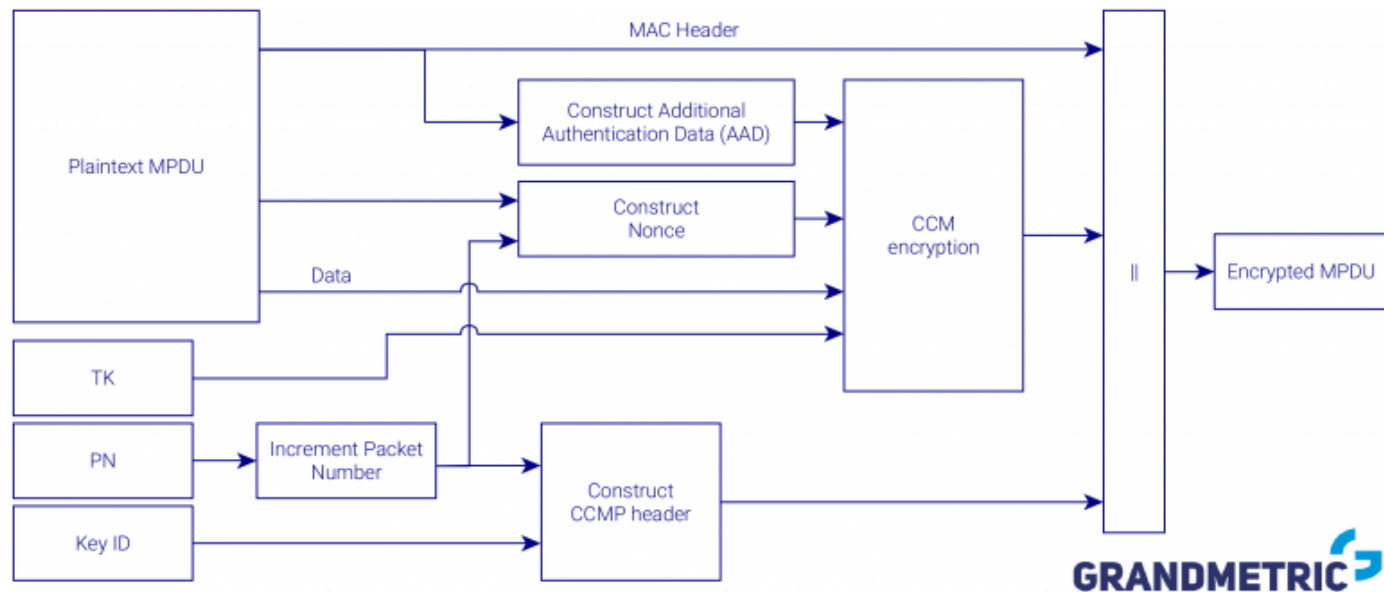
1. Klucze szyfrujące muszą być ręcznie skonfigurowane na każdym z komunikujących się urządzeń. Nastręcza to wiele problemów. Głównym jest zapewnienie poufnego transportu klucza. Często się zdarza, że pracownik korzystający z sieci WLAN dostaje od administratora klucz i sam go sobie wpisuje w konfiguracji karty sieciowej. A co z przypadkiem, gdy ten pracownik odejdzie z firmy? Należałoby zmienić klucz na wszystkich stacjach korzystających z sieci WLAN. Dodatkowo powinna zostać wdrożona (tak jak z innymi hasłami) procedura okresowej zmiany klucza. Jednak najczęstszą praktyką — ze względu na dużą uciążliwość zmiany — jest pozostawianie kluczy bez modyfikacji przez długie miesiące.
2. Wielu administratorów korzysta ze słabszych kluczy 40-bitowych — głównie dlatego, że są łatwiejsze do zapamiętania, gdy trzeba skonfigurować wiele urządzeń.
3. W 2001 roku pojawiły się opracowania naukowe opisujące metody „łamania” kluczy wykorzystujące słabości w algorytmie WEP. Okazało się, że po podsłuchaniu dużej ilości danych (wystarczy ok. 1 – 2 miliony ramek) można za pomocą algorytmów o mniejszej sile obliczeniowej niż użyty do kodowania odkryć klucz WEP. Niebawem pojawiło się darmowe, ogólnodostępne oprogramowanie do wykonywania takich działań.
4. Autoryzacja stacji użytkowników odbywa się poprzez weryfikację adresu MAC. Zmiana adresu MAC stacji radiowej jest dziecinnie prosta, nawet w systemach Windows.
5. Każdy z użytkowników sieci WLAN może podsłuchiwać innych (z różnym skutkiem, w zależności od odległości) transmitujących z tym samym kluczem WEP. WEP nie zabezpiecza przed podsłuchaniem transmisji sąsiada, traktując wszystkich użytkowników sieci bezprzewodowej jak rodzinę.

WiFi - szyfrowanie

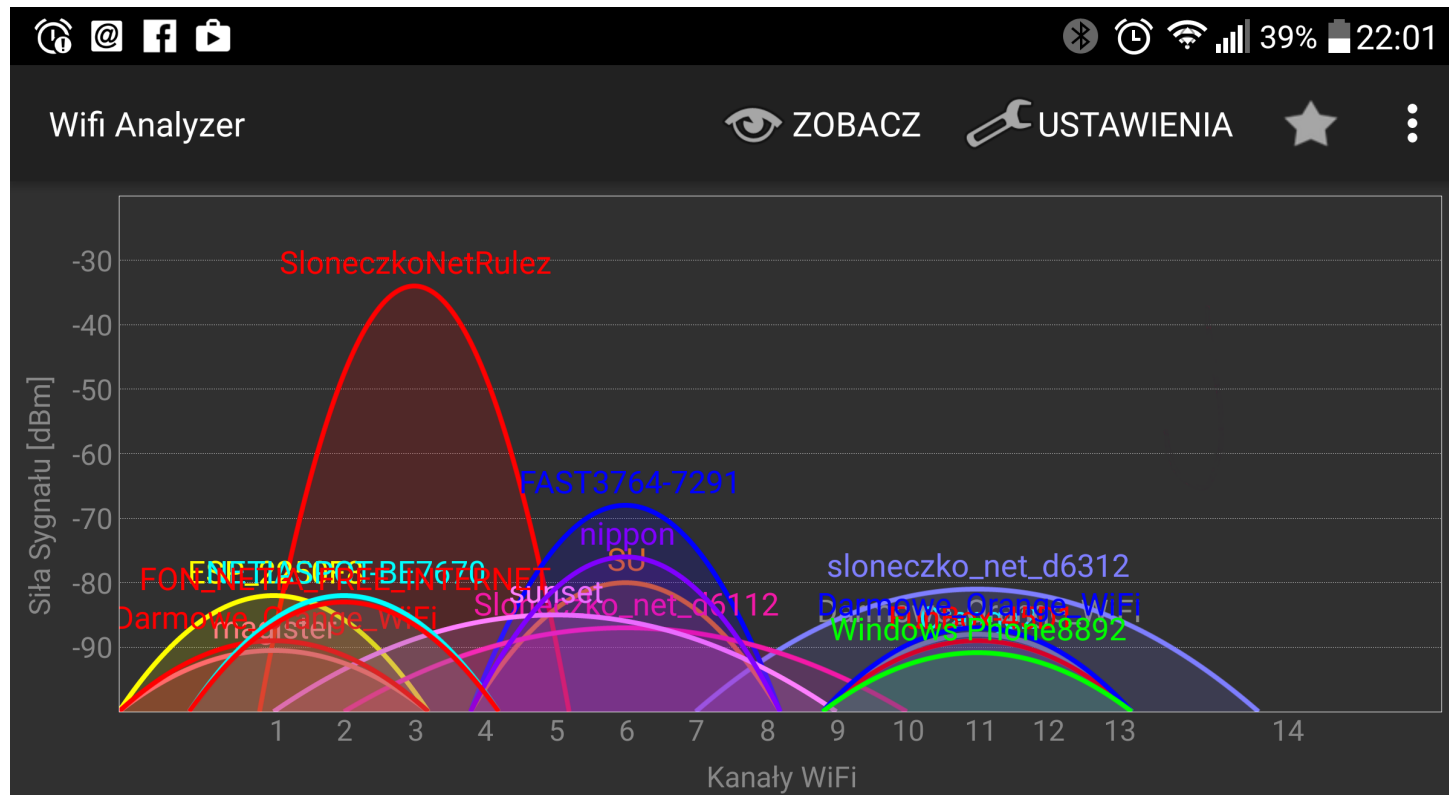
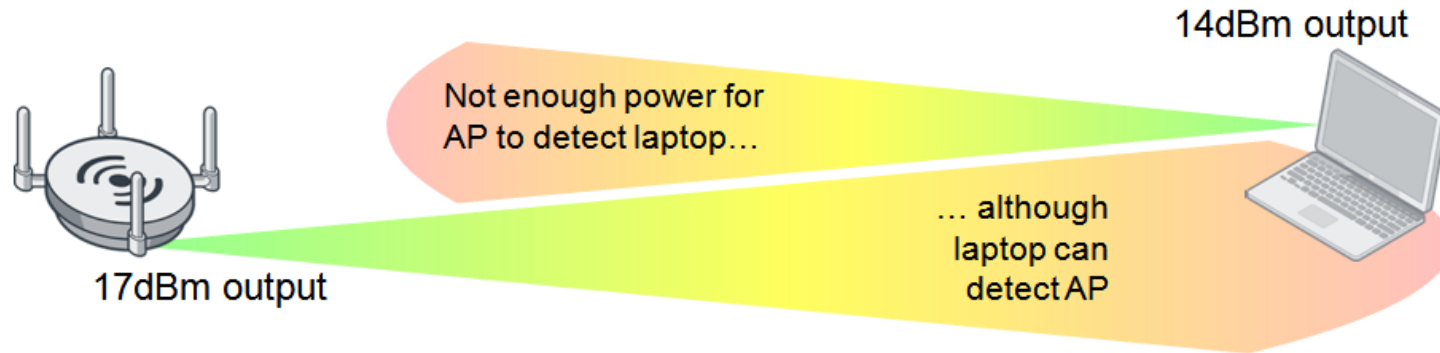
WPA (Wi-Fi Protected Access)



WPA2



WiFi – co robić gdy nie działa?

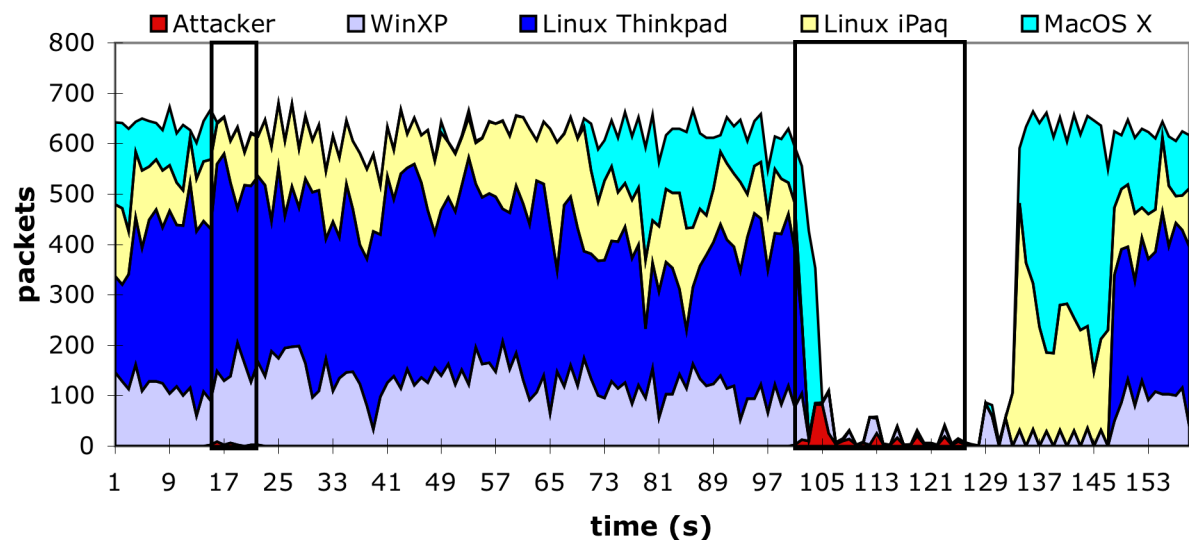


- Sprawdzić zajętość kanałów, sprawdzić moc sygnału, ustawić szyfrowanie aby nikt niepożądany się nie podłączył

WiFi – bezpieczeństwo

- Ze względu na strukturę sieci bezprzewodowych (nie możemy jej ograniczyć jak kabla) są one bardziej podatne na ataki
- Przykładowe typy:
 - **DoS** (*Denial of Service*), ataki odmowy usługi:
 - *zakłócanie* – generowanie zakłóceń utrudniające działanie sieci; trudne do wyeliminowania
 - *flood* – zajęcie wszystkich kanałów
 - *deauthenticate frames* – wysyłanie ramek zrywających połączenie (gdy brak kontroli MAC adresów)

– Spoofing



WiFi – spoofing

<https://niebezpiecznik.pl/post/3-sposoby-na-podsluch-telefonu-komorkowego/>

12:11
26/10/2013

3 sposoby na podsłuch telefonu komórkowego ...i rady jak podsłuchu uniknąć

Autor: Piotr Konieczny | Tagi: Angela Merkel, GSM, IMSI

Catcher, inwigilacja, mobile, NSA, podsłuch, prywatność, służby, SIM, telefonia

2. Podsłuch telefonu na warstwie innych niż GSM protokołów komunikacyjnych, np. poprzez interfejs sieci bezprzewodowych Wi-Fi.

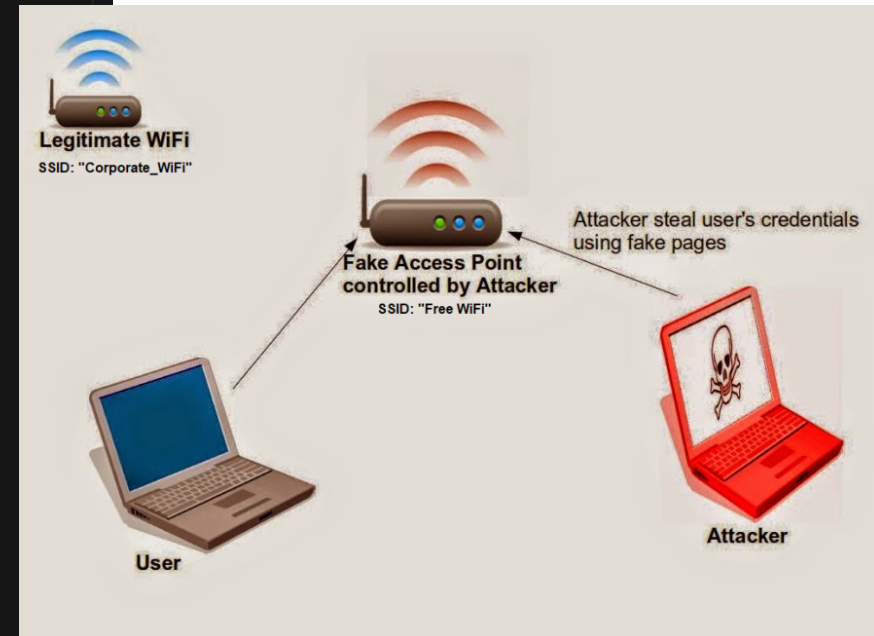
Większość smartphone'ów ma interfejsy Wi-Fi, których użytkownicy nie wyłączają, kiedy przestają korzystać z sieci bezprzewodowej Wi-Fi (wychodzą spoza jej zasięgu). Wtedy taki telefon, np. schowany w kieszeni w trakcie podróży po mieście, co jakiś czas skanuje okolicę w poszukiwaniu SSID znanych mu sieci Wi-Fi ...i jeśli widzi znajomą sieć (np. hotspot w kawiarni, do którego już kiedyś się podłączaliśmy), to **łączy się z nim automatycznie** — a po połączeniu, wiadomo, część aplikacji ożywa; odbiera się poczta, synchronizują się wiadomości na Facebooku, itp.



W tym przypadku atak polega na podstawieniu **fałszywego access-pointa**, który wykrywa próby wyszukiwania przez telefon znanych mu sieci Wi-Fi i błyskawicznie uruchamia fałszywe access pointy o nazwach, których szukał telefon. To sprawia, że telefon myśli, że znalazł "znajomą" sieć i łączy się z fałszywym access pointem. Ten oczywiście podsłuchuje ruch internetowy smartphone'a lub wręcz modyfikuje go aby podsłuch był łatwiejszy, np. zamieniając próby połączeń HTTPS na HTTP (o ile serwer, do którego łączy się podsłuchiwany telefon jest źle skonfigurowany — taki **atak, z wykorzystaniem sslstripa** opisaliśmy na przykładzie warszawskiego Veturilo).

Niebezpiecznik

o bezpieczeństwie i nie...



WiFi – spoofing

<https://niebezpiecznik.pl/post/3-sposoby-na-podsluch-telefonu-komorkowego/>

1. Podsluch telefonu na warstwie protokołów komunikacji GSM.

Podsluchujący podstawia fałszywy BTS (stację bazową), do której podłącza się telefon ofiary. Fałszywą stacją bazową, czyli tzw. **IMSI Catcher**, popularnie zwany “jaskółką” można albo kupić (ale ceny oficjalnych oscylują w okolicy miliona dolarów a ich sprzedaż jest limitowana do służb) albo zrobić **samemu**, m.in. przy pomocy **USRP i OpenBTS**.

Jak działa IMSI Catcher?

Po włączeniu IMSI Catchera, telefony komórkowe w okolicy zauważają, że pojawił się mocniejszy sygnał sieci i przepinają się na fałszywy nadajnik. Fałszywy nadajnik z kolei łączy się z oryginalną siecią, aby przechwycone komórki mogły wykonywać i odbierać połączenia. Jest to klasyczny atak **Man in the middle** — będąc w środku komunikacji, fałszywy BTS wcale nie musi **łamać szyfrowania protokołów sieci GSM**, bo po prostu wymusza brak szyfrowania połączeń, korzystając z tego, iż większość telefonów komórkowych w żaden sposób nie sygnalizuje swojemu właścicielowi, że podłączyło się do sieci GSM bez szyfrowania.

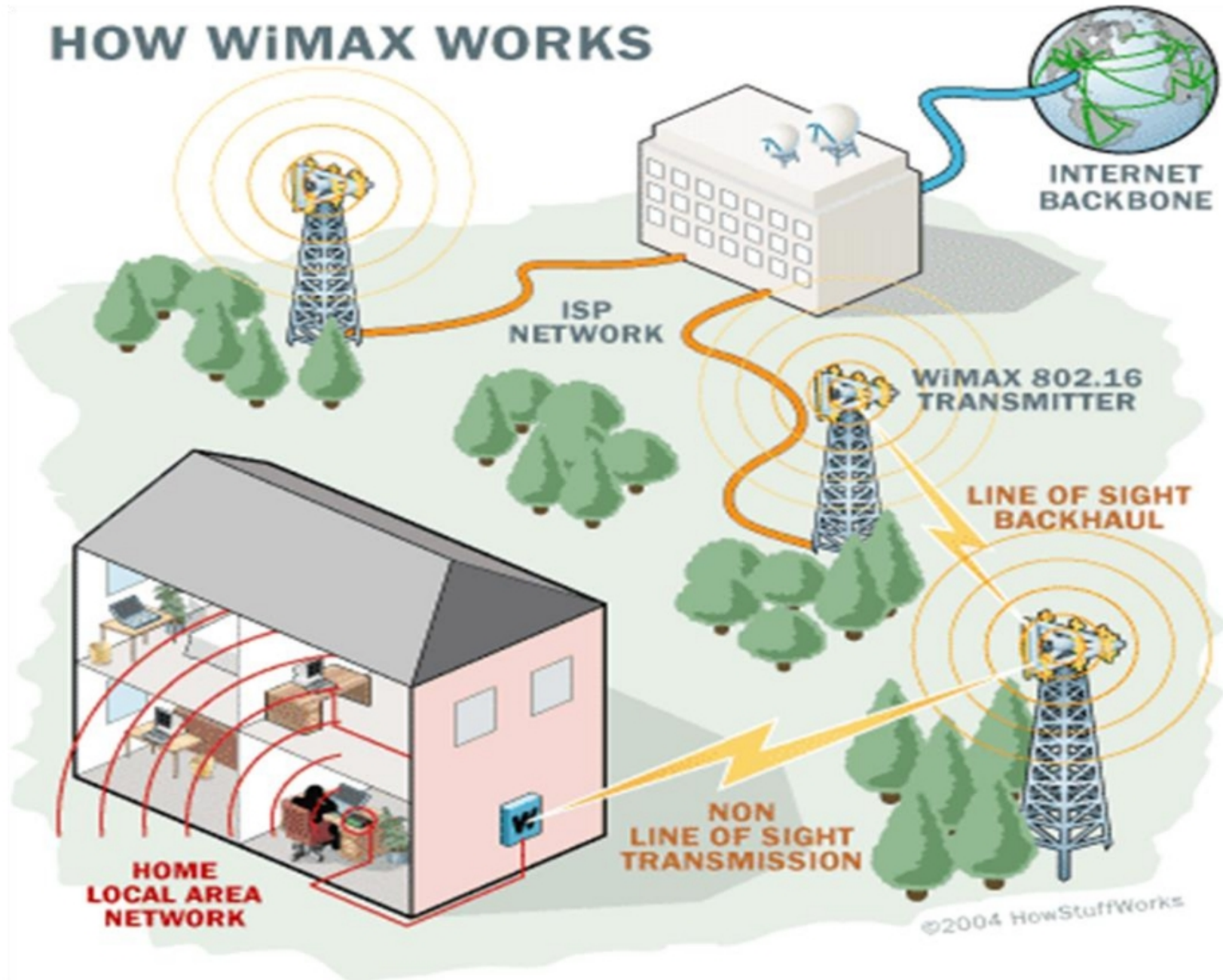
Brak szyfrowania pozwala fałszywemu BTS-owi na podsłuchiwanie rozmów, SMS-ów, transmisji pakietowej (internet). Podsłuchiwane połączenia można oczywiście nagrywać. Dodatkowymi funkcjami fałszywego BTS-a jest korelacja danych, czyli możliwość namierzenia osoby, która zmieniła telefon (ale korzysta z tej samej karty) lub zmieniła kartę SIM (ale korzysta z tego samego telefonu) lub zmieniła kartę SIM i telefon jednocześnie (ale dalej wykonuje połączenia na te same numery).



iPhone – reakcja na podpięcie się do BTS bez szyfrowania



Budowa sieci bezprzewodowych



Sieci bezprzewodowe

Access point WiFi

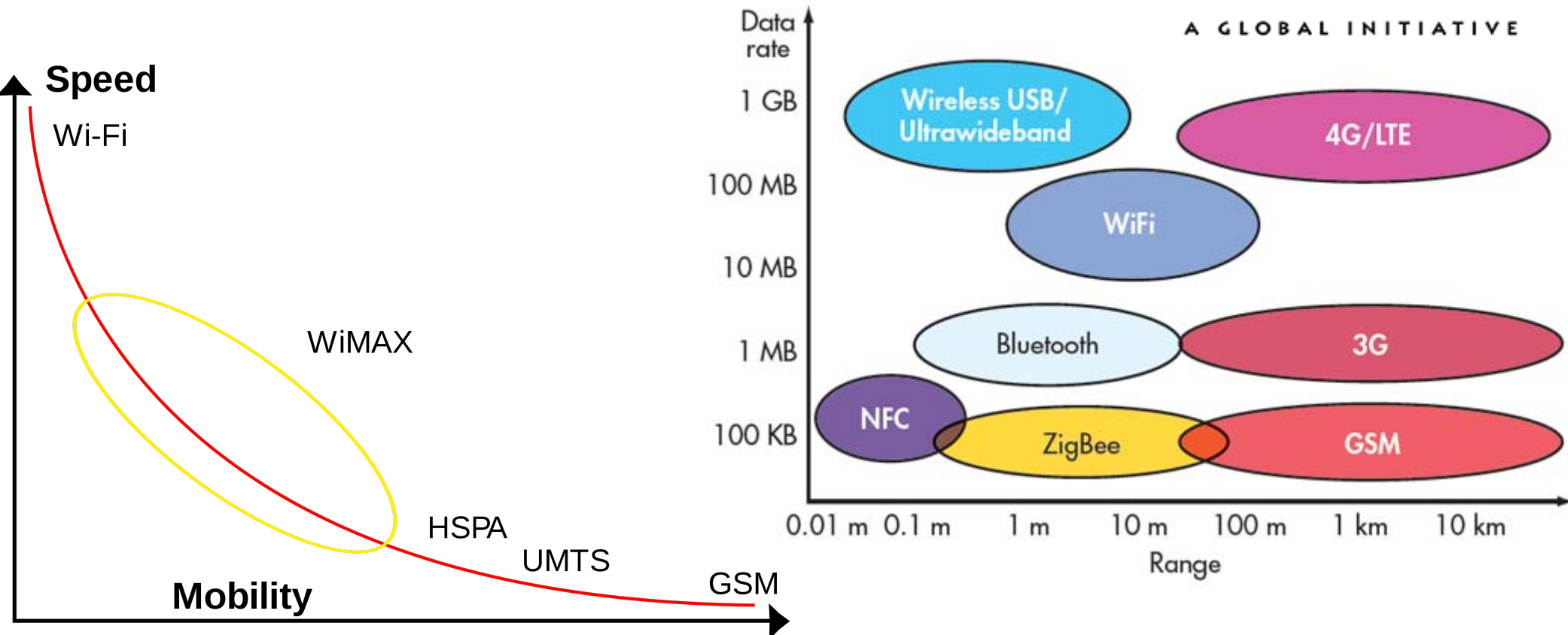


Stacja bazowa WiMAX





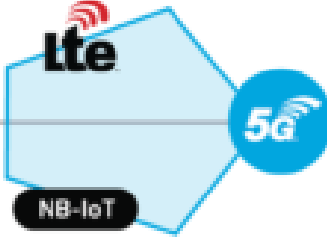
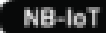
Sieci bezprzewodowe

- Istnieją też standardy zdefiniowane w innych organizacjach niż IEEE
- Przykładowo standardy komórkowe zarządzane są przez **3rd Global Partnership Project (3GPP)**



Sieci bezprzewodowe

- Standardy się częściowo przekrywają, czasami konkurują, ale również uzupełniają – w zależności od potrzeby i warunków
 - zasięgu, prędkości przesyłu danych, energochłonności, ruchliwości nadajników i odbiorników względem siebie

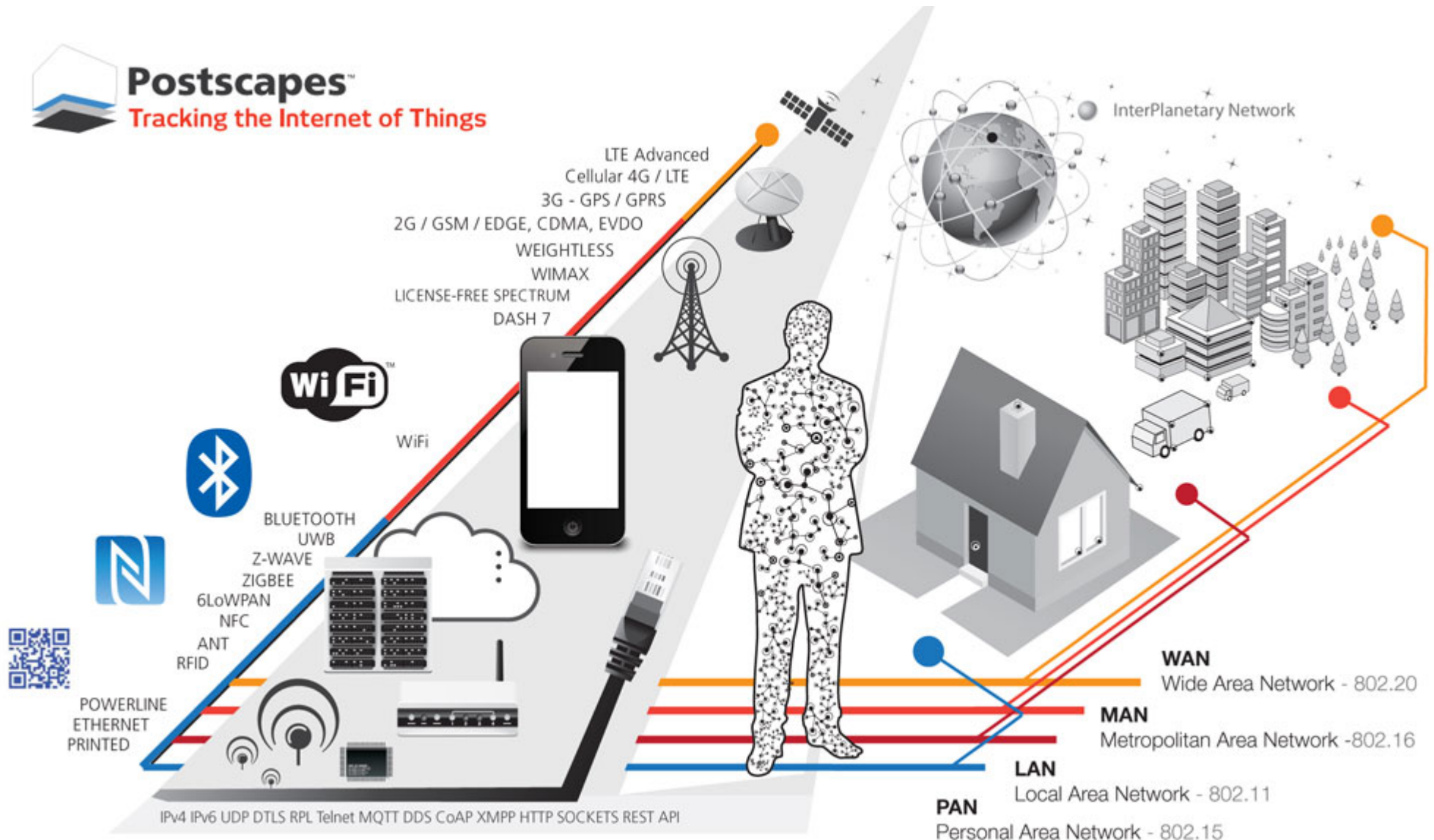
	 Wearables	 Home	 Phone
Range (typical)	<10m/30ft	<100m/300ft	Outdoor (Km/miles)
Content	 Bluetooth	 WiFi	
Sense & control	 Bluetooth SMART	 zigbee	
Typical applications	Personal appliances (wristband, smart watch, step counter, keyboard, mouse, pointer, etc.)	Indoor networks (Internet, email, phone, security, energy management, home monitoring, etc.)	Outdoor networks (phone, chat, Internet, smart city, industry 4.0, agriculture, smart logistics, etc.)

QORVO

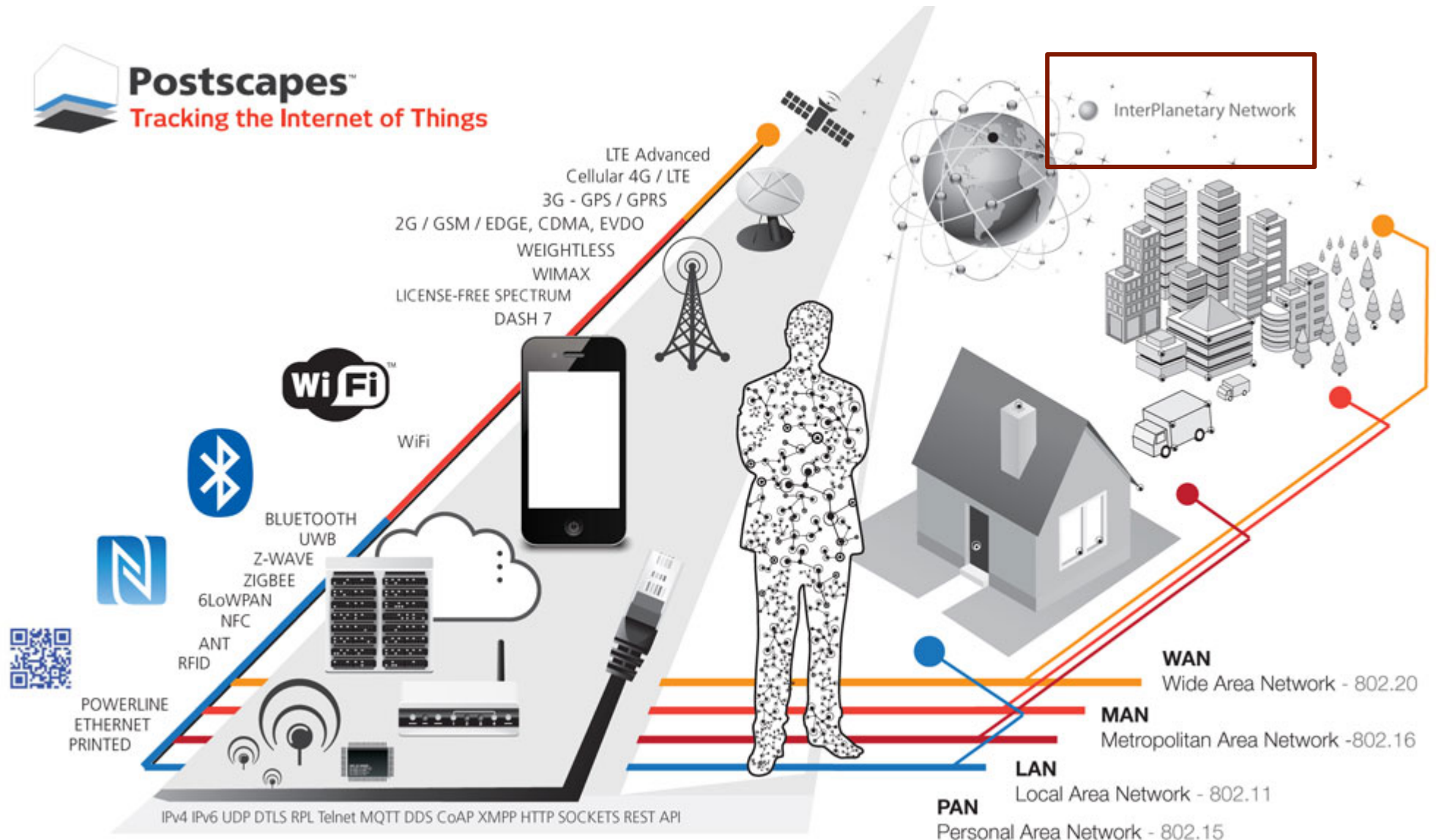
©2018 Qorvo, Inc.

Internet of Things

- Internet of Things (IoT) – różne, często nieoczywiste przedmioty mogą wymieniać dane

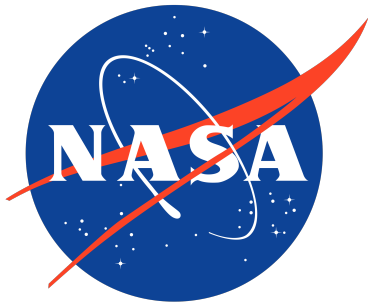
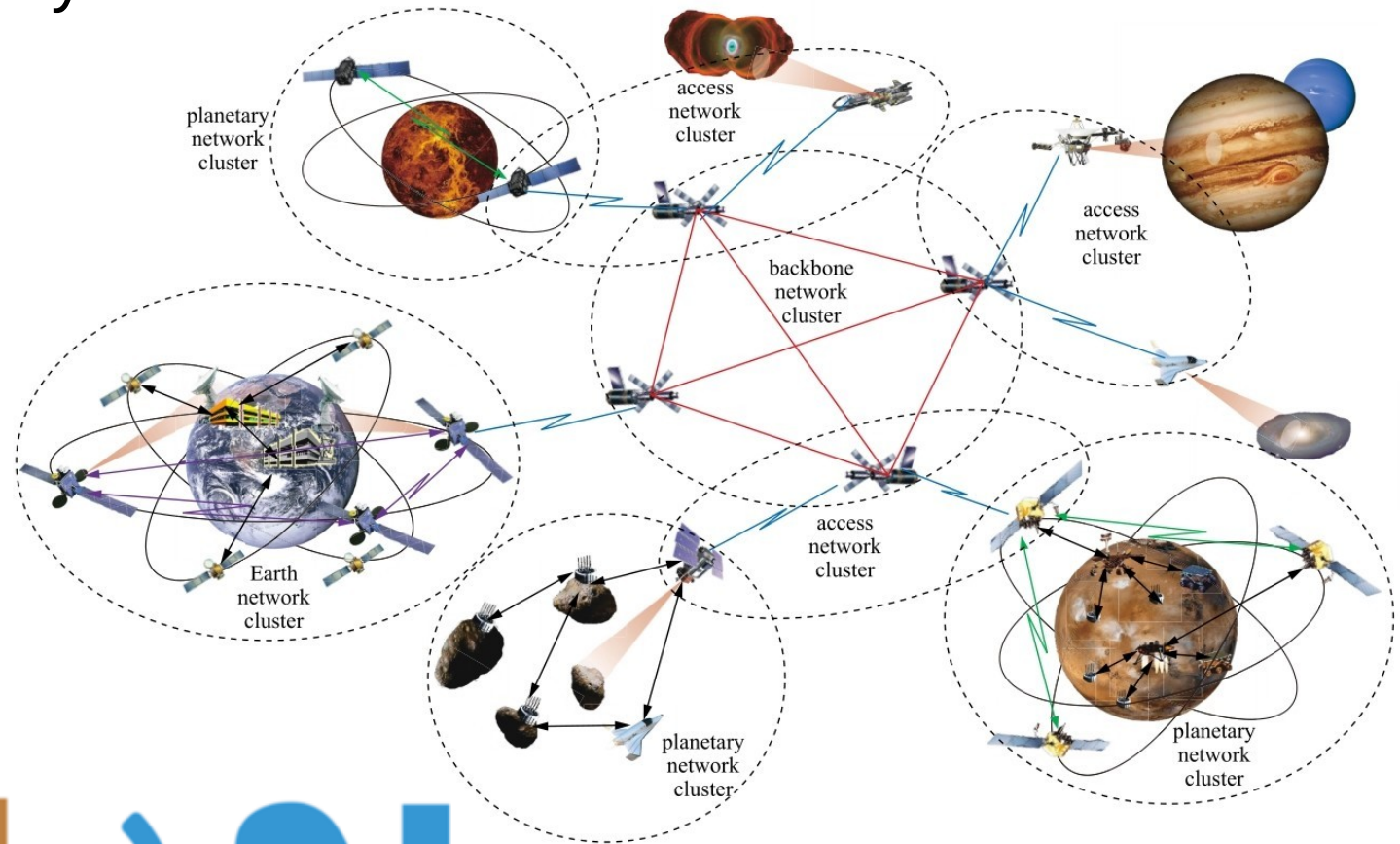


InterPlanetary Network



InterPlanetary Network

- **InterPlanetary Network** – tworzenie standardu i technologii umożliwiających komunikację Internetową z innymi planetami, statkami kosmicznymi





KONIEC