Sieci bezprzewodowe

Bartosz Chodorowski

<chomzee@ethernet.pl>

Anatomia PC, 19 marca 2009

1. Bezprzewodowa transmisja radiowa
   - Moc, waty, decybele
   - Łącza radiowe
   - Kable
   - Anteny
   - Odbiorniki, nadajniki
2. Standardy, protokoły
   - Topologie, tryby pracy
   - WLAN – IEEE 802.11
   - Inne IEEE 802.11*
3. Bezpieczeństwo
   - Namiastka bezpieczeństwa
   - WEP
   - WPA
   - WPA2
   - Obrona w wyższych warstwach

Wat, miliwat, decybel, dBm

- W (wat) – jednostka mocy

Wat, miliwat, decybel, dBm

- W (wat) – jednostka mocy
- mW (miliwat) – $1000mW = 1W$

Wat, miliwat, decybel, dBm

- W (wat) – jednostka mocy
- mW (miliwat) – $1000mW = 1W$
- dB (decybel) – jednostka logarytmiczna

$$P[dB] = 10 \cdot log_{10}\left(\frac{P[W]}{1W}\right)$$

Wat, miliwat, decybel, dBm

- W (wat) – jednostka mocy
- mW (miliwat) – $1000mW = 1W$
- dB (decybel) – jednostka logarytmiczna

$$P[dB] = 10 \cdot log_{10}\left(\frac{P[W]}{1W}\right)$$

- dBm – decybel odniesiony do 1mW

$$P[dBm] = 10 \cdot log_{10}\left(\frac{P[mW]}{1mW}\right)$$

dBi

- dBi – jednostka miary zysku anteny

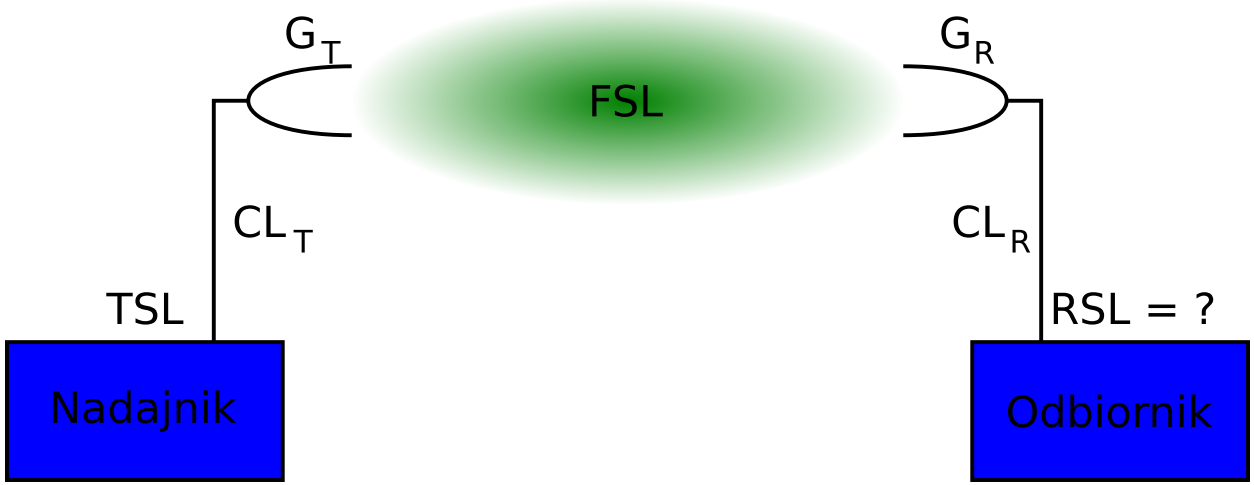
dBi

- dBi – jednostka miary zysku anteny
- Mówi o tym, o ile dB poziom sygnału jest większy w stosunku do anteny izotropowej

dBi

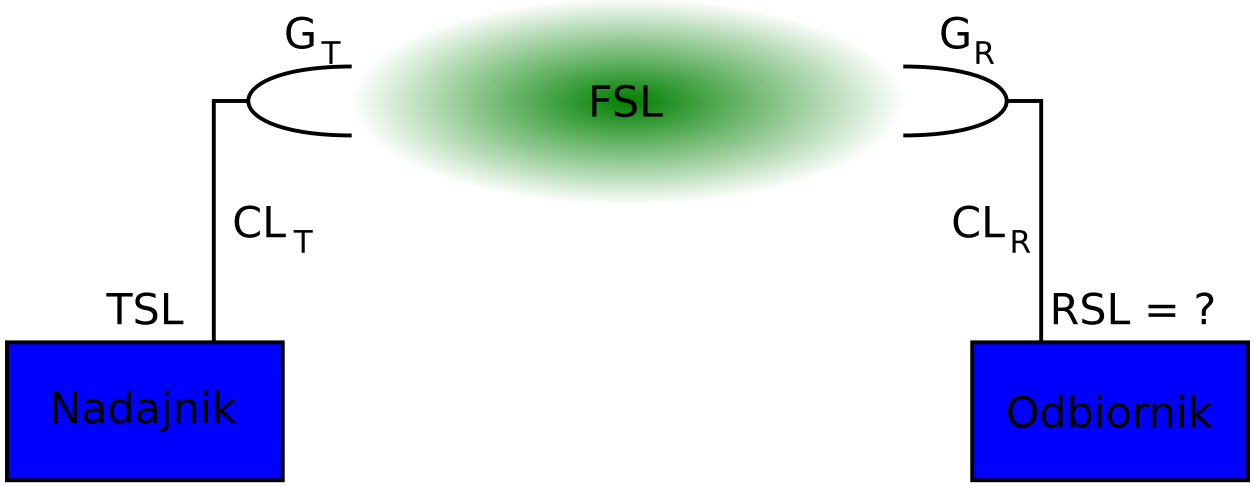
- dBi – jednostka miary zysku anteny
- Mówi o tym, o ile dB poziom sygnału jest większy w stosunku do anteny izotropowej
- Antena izotropowa – teoretyczna antena, która emituje energię jednakowo we wszystkich kierunkach

Energetyczny bilans łącza radiowego, cz. 1



$TSL[dBm]$	–	poziom sygnału (moc) nadajnika
$CL_T[dB]$	–	straty sygnału w przewodzie
$G_T[dBi]$	–	zysk anteny nadawczej
$FSL[dB]$	–	tłumienie wolnej przestrzeni
$G_R[dBi]$	–	zysk anteny odbiorczej
$CL_R[dB]$	–	straty sygnału w przewodzie
$RSL[dBm]$	–	poziom sygnału odbieranego

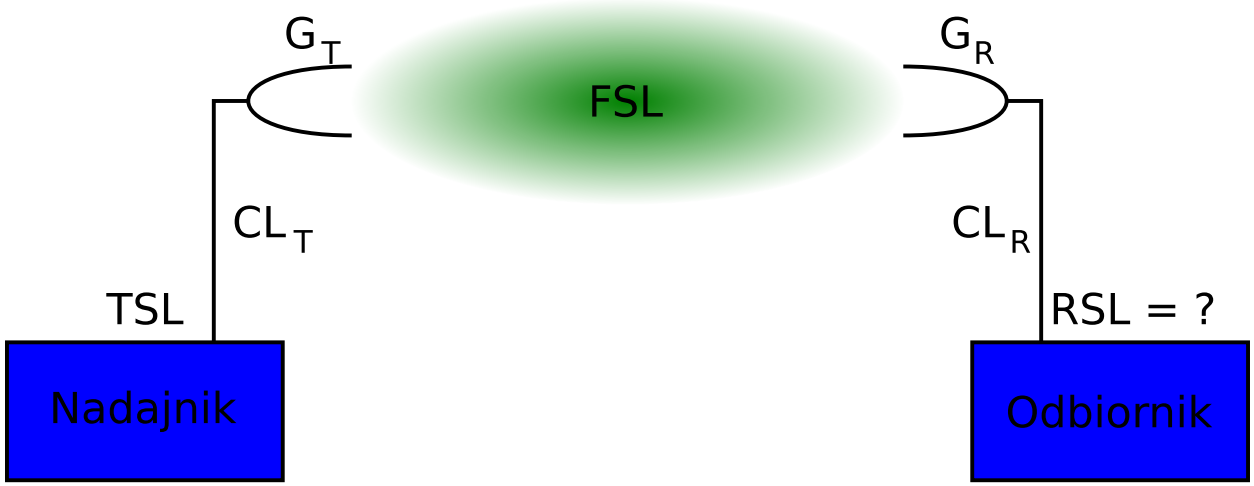
Energetyczny bilans łącza radiowego, cz. 2



$$RSL = TSL - CL_T + G_T - FSL + G_R - CL_R - \alpha$$

Gdzie: α – parametr korekcyjny (do 3 dB)

Energetyczny bilans łącza radiowego, cz. 2

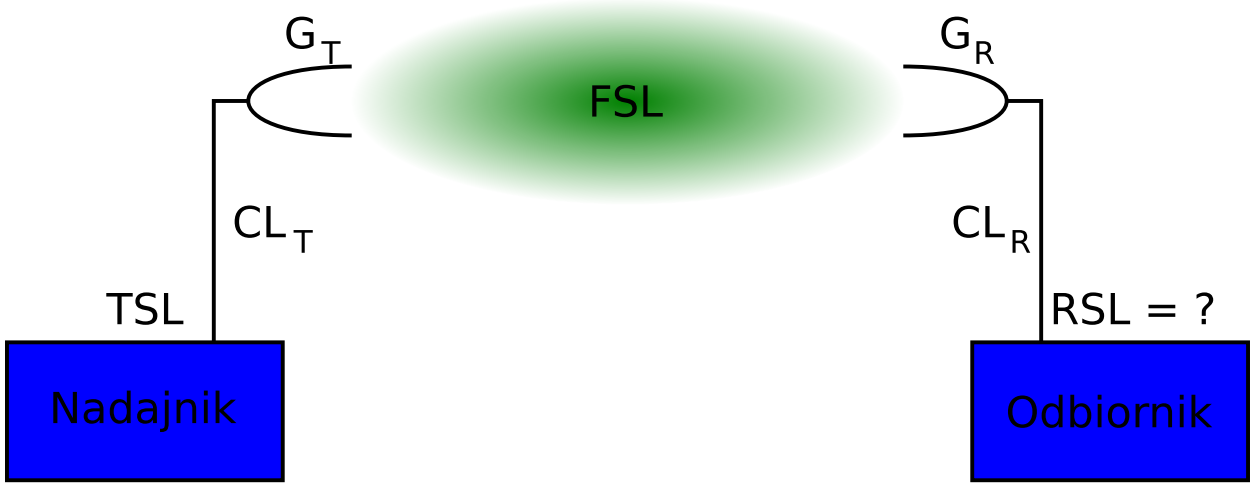


$$RSL = TSL - CL_T + G_T - FSL + G_R - CL_R - \alpha$$

Gdzie: α – parametr korekcyjny (do 3 dB)

Cel:

Energetyczny bilans łącza radiowego, cz. 2



$$RSL = TSL - CL_T + G_T - FSL + G_R - CL_R - \alpha$$

Gdzie: α – parametr korekcyjny (do 3 dB)

Cel:

Uzyskać około $RSL \geq -80\ dBm$ (czułość odbiornika)

EIRP

- (ang. *Effective Isotropical Radiated Power*)

EIRP

- (ang. *Effective Isotropical Radiated Power*)
- Wymogi prawne

EIRP

- (ang. *Effective Isotropical Radiated Power*)
- Wymogi prawne
- $EIRP[dBm] = TSL - CL_T + G_T$

EIRP

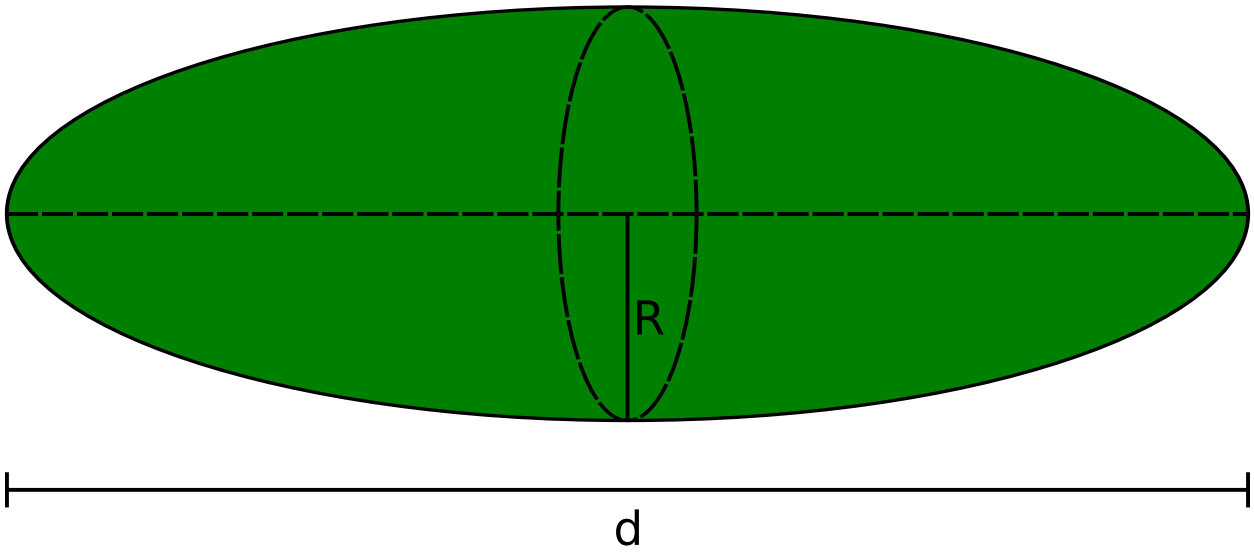
- (ang. *Effective Isotropical Radiated Power*)
- Wymogi prawne
- $EIRP[dBm] = TSL - CL_T + G_T$
- $EIRP \leq 20dBm$ (dla 2,4 GHz)

EIRP

- (ang. *Effective Isotropical Radiated Power*)
- Wymogi prawne
- $EIRP[dBm] = TSL - CL_T + G_T$
- $EIRP \leq 20dBm$ (dla 2,4 GHz)
- $EIRP \leq 30dBm$ (dla 5 GHz)

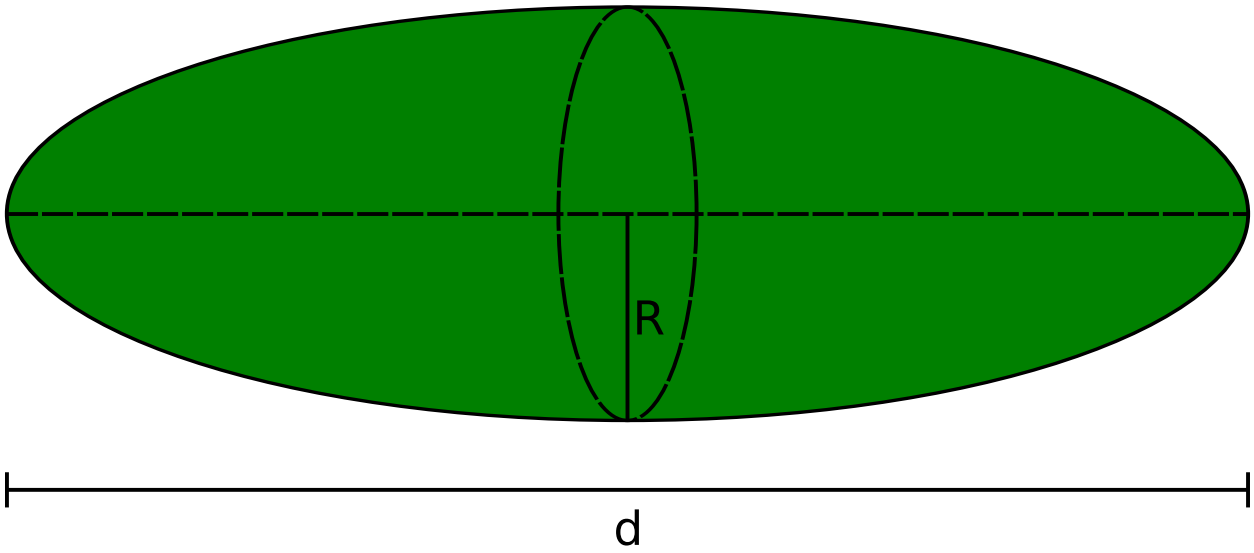
1 strefa Fresnela

Przestrzeń aktywnie biorąca udział w przenoszeniu energii sygnału.



1 strefa Fresnela

Przestrzeń aktywnie biorąca udział w przenoszeniu energii sygnału.



$$R[m] = 17,3\sqrt{\frac{d_1 d_2}{df}}$$

$$d[km] = d_1 + d_2 \qquad f[GHz]$$

Tłumienie wolnej przestrzeni, model FSL

- Model FSL jest przydatny do oszacowania tłumienia wolnej przestrzeni

Tłumienie wolnej przestrzeni, model FSL

- Model FSL jest przydatny do oszacowania tłumienia wolnej przestrzeni
- Założenia:
  - między nadajnikiem a odbiornikiem nie ma przeszkód
  - do odbiornika nie dochodzą fale odbite
  - nie jest przysłonięta 1 strefa Fresnela
  - brak zakłóceń zewnętrznych

Tłumienie wolnej przestrzeni, model FSL

- Model FSL jest przydatny do oszacowania tłumienia wolnej przestrzeni
- Założenia:
  - między nadajnikiem a odbiornikiem nie ma przeszkód
  - do odbiornika nie dochodzą fale odbite
  - nie jest przysłonięta 1 strefa Fresnela
  - brak zakłóceń zewnętrznych
- dla częstotliwości 2,4 GHz: $FSL[dB] = 100 + 20log_{10}d$

Tłumienie wolnej przestrzeni, model FSL

- Model FSL jest przydatny do oszacowania tłumienia wolnej przestrzeni
- Założenia:
  - między nadajnikiem a odbiornikiem nie ma przeszkód
  - do odbiornika nie dochodzą fale odbite
  - nie jest przysłonięta 1 strefa Fresnela
  - brak zakłóceń zewnętrznych
- dla częstotliwości 2,4 GHz: $FSL[dB] = 100 + 20log_{10}d$
- dla częstotliwości 5 GHz: $FSL[dB] = 106 + 20log_{10}d$

Kable

- Skrętka?

Kable

- Skrętka?
  NIE!

Kable

- Skrętka?
  NIE!
- Kabel koncentryczny!

Kable

- Skrętka?
  NIE!
- Kabel koncentryczny!

Nadaje się do przekazywania sygnału wysokiej częstotliwości

Kable

- Skrętka?
  NIE!
- Kabel koncentryczny!

  Nadaje się do przekazywania sygnału wysokiej częstotliwości
- Tłumienność:
  40-50 $\frac{dB}{100m}$ (2,4 GHz)
  60-70 $\frac{dB}{100m}$ (5 GHz)

Kable

- Skrętka?
  NIE!
- Kabel koncentryczny!

  Nadaje się do przekazywania sygnału wysokiej częstotliwości
- Tłumienność:
  40-50 $\frac{dB}{100m}$ (2,4 GHz)
  60-70 $\frac{dB}{100m}$ (5 GHz)
- Dla porównania – nowoczesny światłowód: $0,2\frac{dB}{km}$

Parametry anten

- charakterystyka promieniowania

Parametry anten

- charakterystyka promieniowania
  - kierunkowe

Parametry anten

- charakterystyka promieniowania
  - kierunkowe
  - dookolne

Parametry anten

- charakterystyka promieniowania
  - kierunkowe
  - dookolne
  - sektorowe

Parametry anten

- charakterystyka promieniowania
  - kierunkowe
  - dookolne
  - sektorowe
  - paraboliczne

Parametry anten

- charakterystyka promieniowania
  - kierunkowe
  - dookolne
  - sektorowe
  - paraboliczne
- zysk

Parametry anten

- charakterystyka promieniowania
  - kierunkowe
  - dookolne
  - sektorowe
  - paraboliczne
- zysk
- impedancja

Parametry anten

- charakterystyka promieniowania
  - kierunkowe
  - dookolne
  - sektorowe
  - paraboliczne
- zysk
- impedancja
- polaryzacja

Parametry anten

- charakterystyka promieniowania
  - kierunkowe
  - dookolne
  - sektorowe
  - paraboliczne
- zysk
- impedancja
- polaryzacja
- pasmo

Anteny kierunkowe

Anteny kierunkowe

- określony kierunek

Anteny kierunkowe

- określony kierunek
- większy kąt apertury = mniejszy zysk

Anteny dookolne

Anteny dookolne

- kąt apertury: 360°

Anteny dookolne

- kąt apertury: 360^o
- promieniowanie w płaszczyźnie poziomej

Anteny sektorowe (szczelinowe)

Anteny sektorowe (szczelinowe)

- poziomo: 2×120^o

Anteny sektorowe (szczelinowe)

- poziomo: 2×120^o
- większy kąt promieniowania pionowego

Anteny paraboliczne

Anteny paraboliczne

- bardzo mały kąt apertury

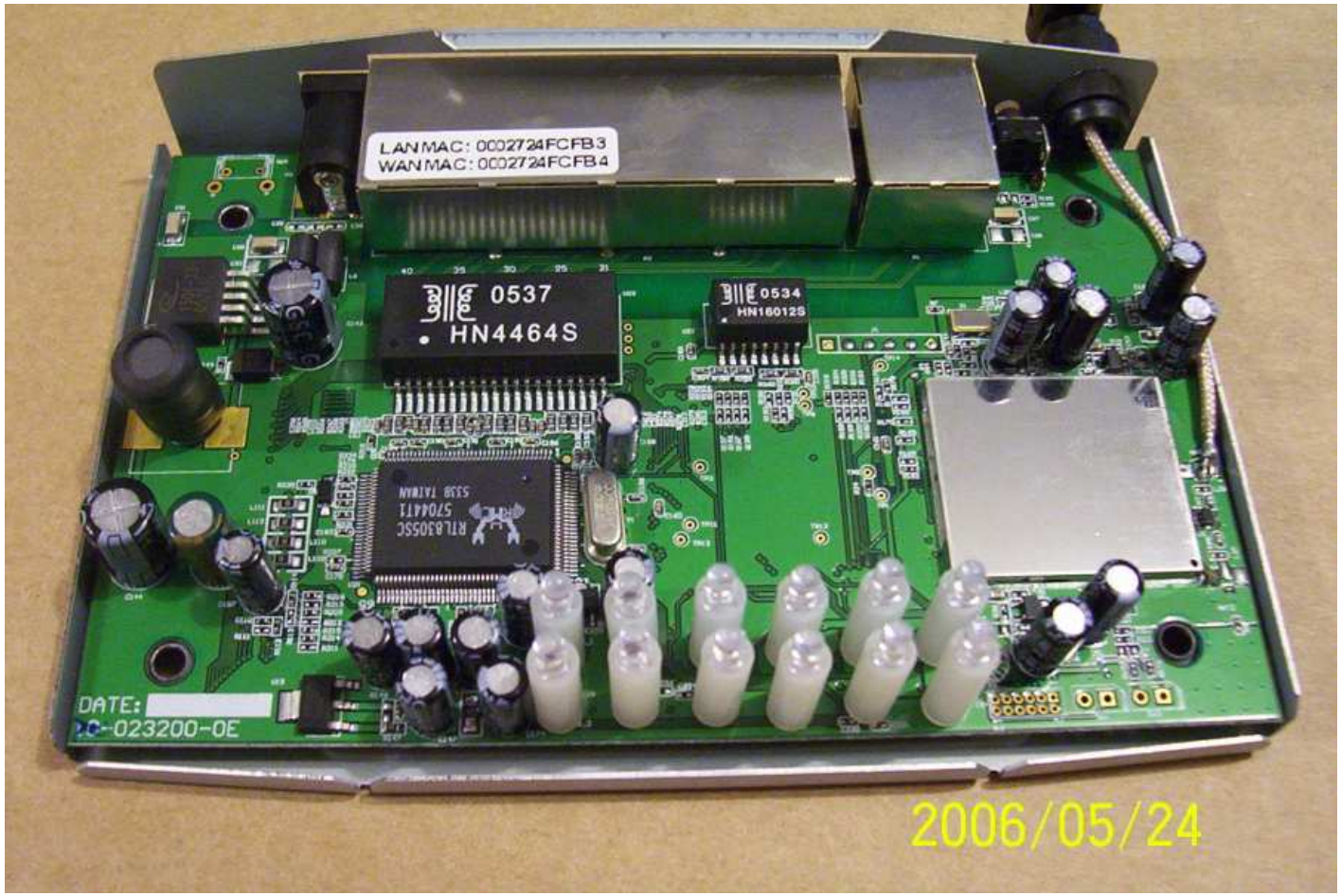
Anteny paraboliczne

- bardzo mały kąt apertury
- duży zysk

Anteny Pringles :-)

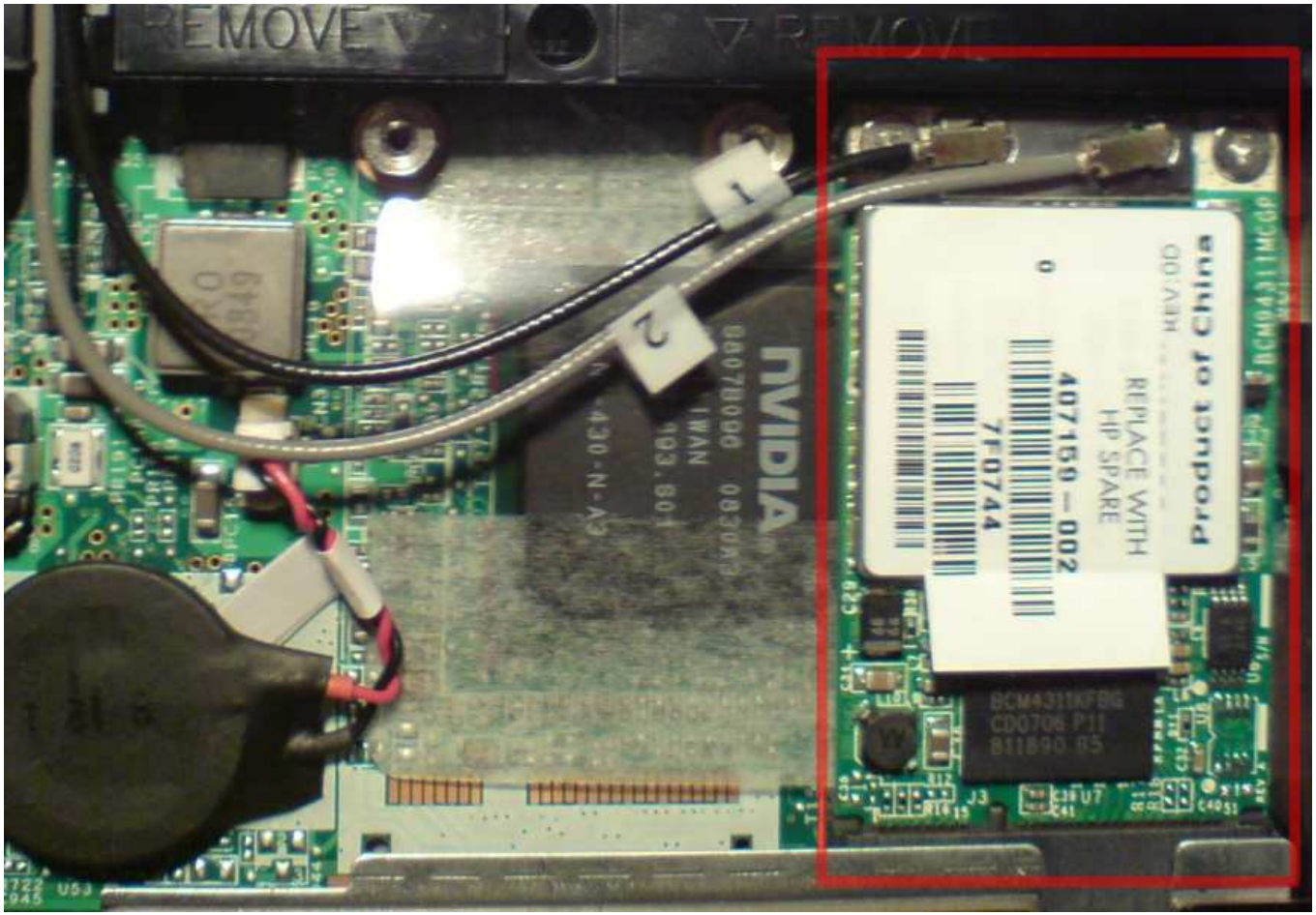
Anteny Pringles :-)

Access Point



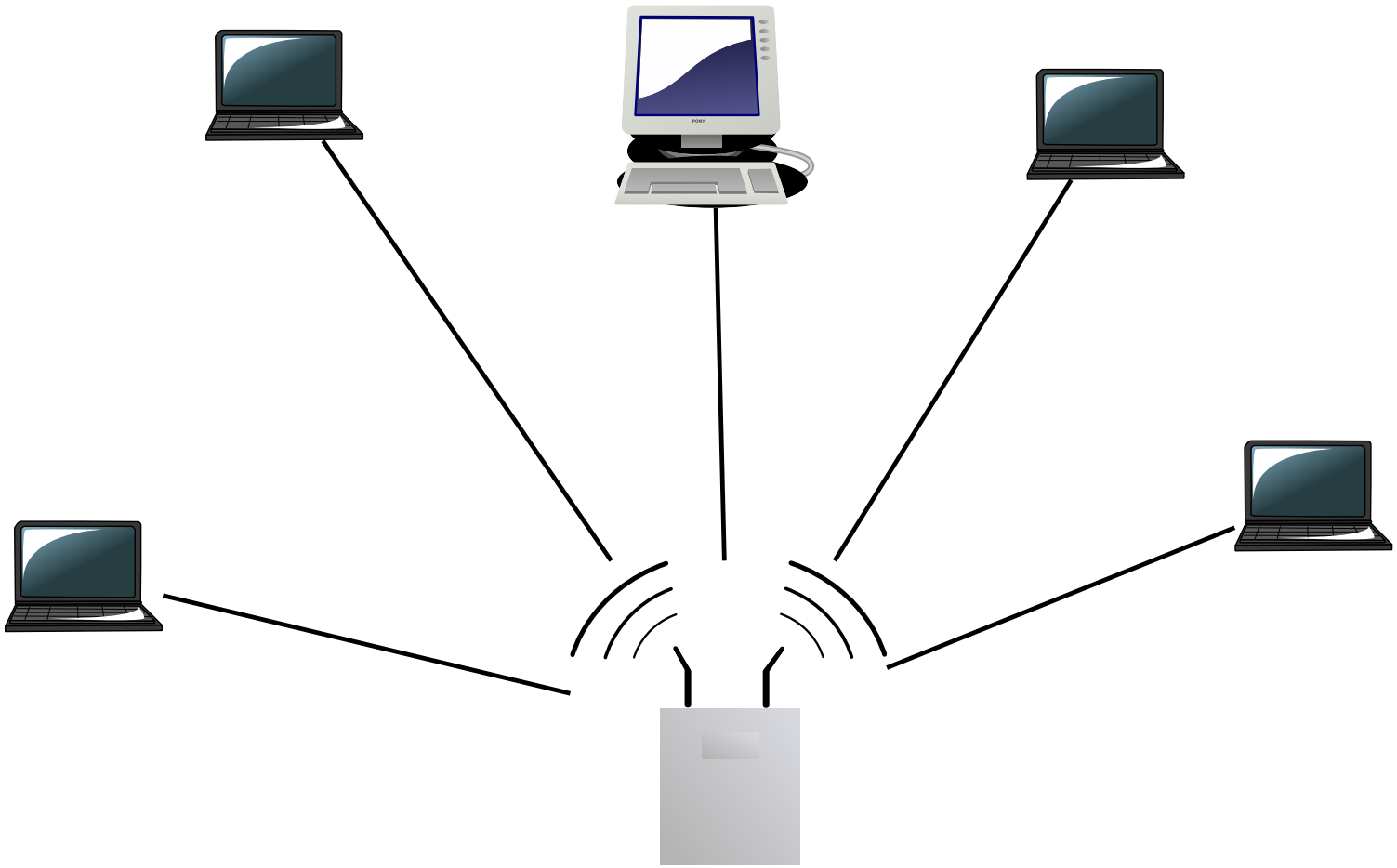
Karta na złącze PCI

Karta na złącze mini-PCI (laptop)

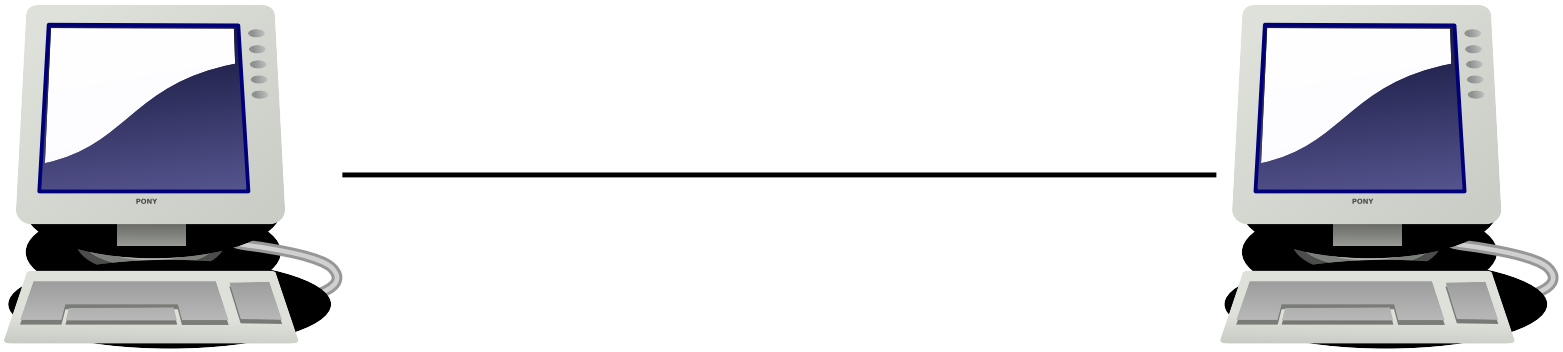


Antena w laptopie

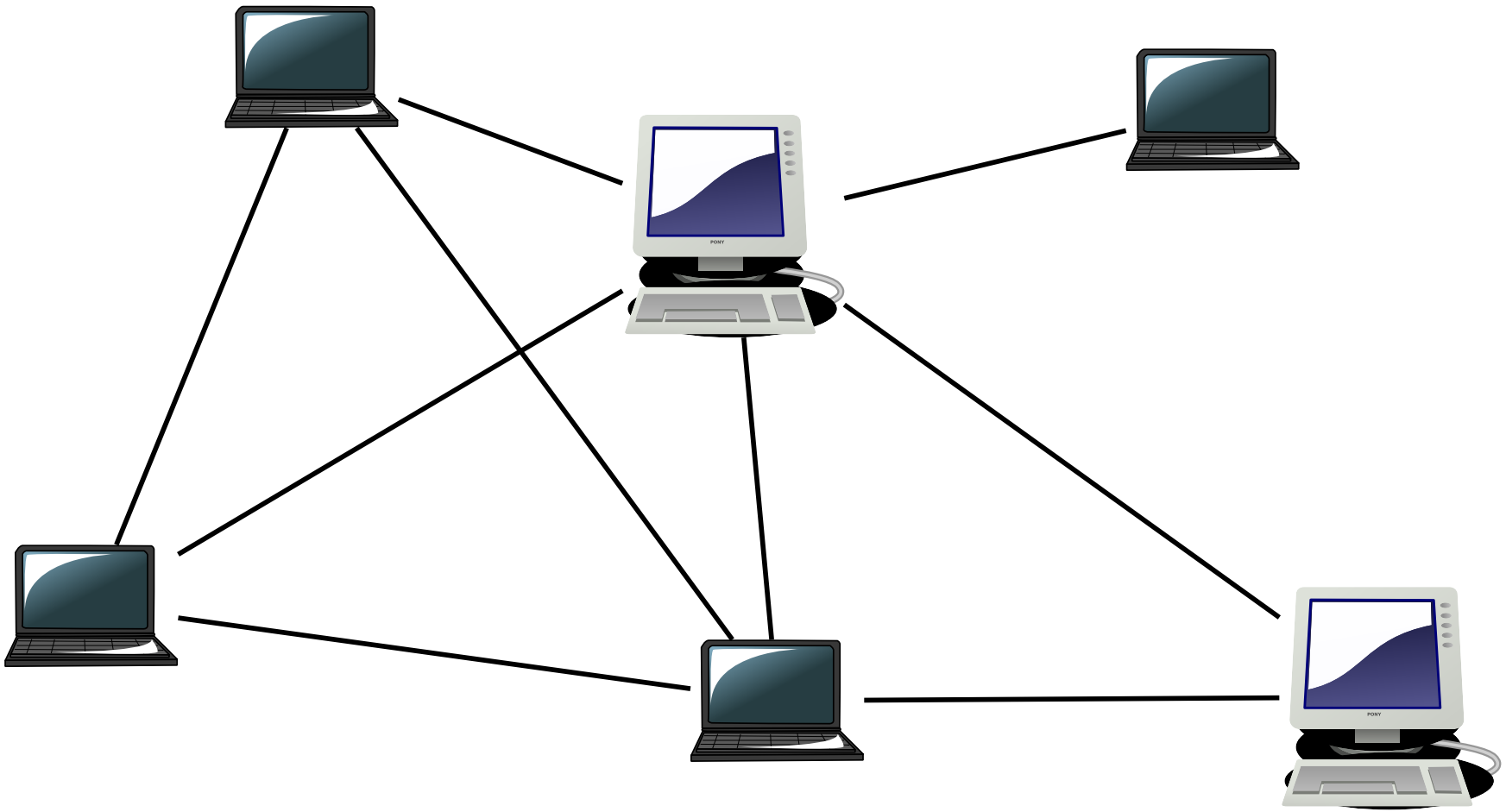
Managed mode / AP mode



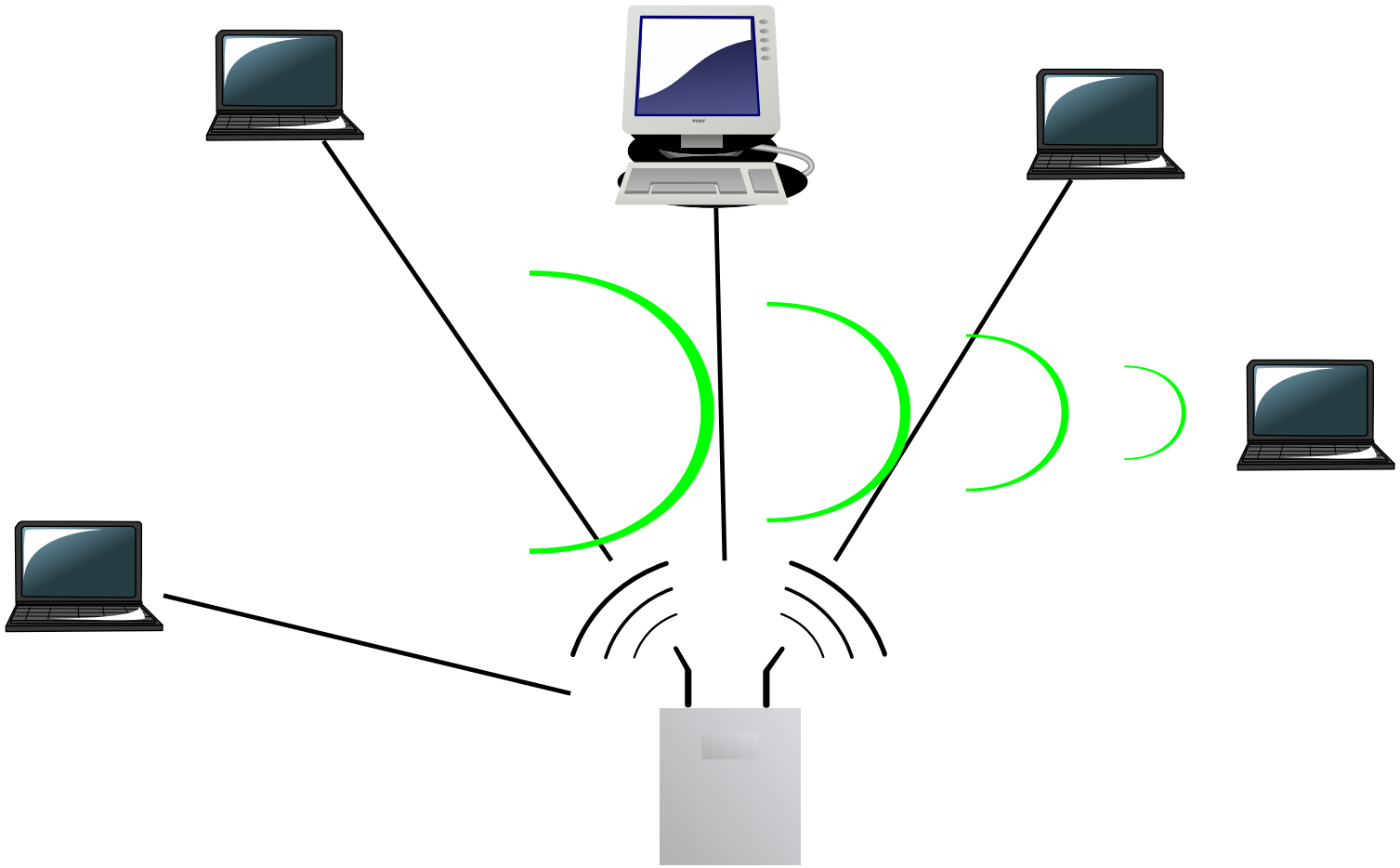
punkt-punkt



Ad-Hoc



Monitor mode



WLAN – IEEE 802.11

- Pierwotny standard
- Standard b
- Standard a
- Standard g
- Standard n

Pierwotny standard – IEEE 802.1y

- Czerwiec 1997

Pierwotny standard – IEEE 802.1y

- Czerwiec 1997
- 2,4 GHz

Pierwotny standard – IEEE 802.1y

- Czerwiec 1997
- 2,4 GHz
- 1, 2 Mb/s

IEEE 802.11b

- Wrzesień 1999

IEEE 802.11b

- Wrzesień 1999
- 2,4 GHz

IEEE 802.11b

- Wrzesień 1999
- 2,4 GHz
- do 11 Mb/s

IEEE 802.11b

- Wrzesień 1999
- 2,4 GHz
- do 11 Mb/s
- 13 kanałów

IEEE 802.11a

- Wrzesień 1999

IEEE 802.11a

- Wrzesień 1999
- 5 GHz

IEEE 802.11a

- Wrzesień 1999
- 5 GHz
- do 54 Mb/s

IEEE 802.11a

- Wrzesień 1999
- 5 GHz
- do 54 Mb/s
- 12 niezachodzących kanałów

IEEE 802.11a

- Wrzesień 1999
- 5 GHz
- do 54 Mb/s
- 12 niezachodzących kanałów
- Stosunkowo duży pobór mocy

IEEE 802.11g

- Czerwiec 2003

IEEE 802.11g

- Czerwiec 2003
- 2,4 GHz

IEEE 802.11g

- Czerwiec 2003
- 2,4 GHz
- do 54 Mb/s

IEEE 802.11g

- Czerwiec 2003
- 2,4 GHz
- do 54 Mb/s
- zgodny ze standardem b

IEEE 802.11g

- Czerwiec 2003
- 2,4 GHz
- do 54 Mb/s
- zgodny ze standardem b
- Super-G

IEEE 802.11n

- Zapowiadany na czerwiec 2010

IEEE 802.11n

- Zapowiadany na czerwiec 2010
- 2,4 lub 5 GHz

IEEE 802.11n

- Zapowiadany na czerwiec 2010
- 2,4 lub 5 GHz
- do **300 Mb/s**

IEEE 802.11n

- Zapowiadany na czerwiec 2010
- 2,4 lub 5 GHz
- do **300 Mb/s**
- MIMO – kilka anten do nadawania/odboiru, wiele kanałów

Inne IEEE 802.11*

- IEEE 802.11c – mosty pomiędzy sieciami

Inne IEEE 802.11*

- IEEE 802.11c – mosty pomiędzy sieciami
- IEEE 802.11d – łączność w poszczególnych krajach

Inne IEEE 802.11*

- IEEE 802.11c – mosty pomiędzy sieciami
- IEEE 802.11d – łączność w poszczególnych krajach
- IEEE 802.11e – QoS

Inne IEEE 802.11*

- IEEE 802.11c – mosty pomiędzy sieciami
- IEEE 802.11d – łączność w poszczególnych krajach
- IEEE 802.11e – QoS
- IEEE 802.11f – roaming przy pomocy protokołu IAPP

Inne IEEE 802.11*

- IEEE 802.11c – mosty pomiędzy sieciami
- IEEE 802.11d – łączność w poszczególnych krajach
- IEEE 802.11e – QoS
- IEEE 802.11f – roaming przy pomocy protokołu IAPP
- IEEE 802.11h – europejski odpowiednik 802.11a

Inne IEEE 802.11*

- IEEE 802.11c – mosty pomiędzy sieciami
- IEEE 802.11d – łączność w poszczególnych krajach
- IEEE 802.11e – QoS
- IEEE 802.11f – roaming przy pomocy protokołu IAPP
- IEEE 802.11h – europejski odpowiednik 802.11a
- IEEE 802.11i – WPA2

Inne IEEE 802.11*

- IEEE 802.11c – mosty pomiędzy sieciami
- IEEE 802.11d – łączność w poszczególnych krajach
- IEEE 802.11e – QoS
- IEEE 802.11f – roaming przy pomocy protokołu IAPP
- IEEE 802.11h – europejski odpowiednik 802.11a
- IEEE 802.11i – WPA2
- IEEE 802.11j – japoński odpowiednik 802.11a

Namiastka bezpieczeństwa

- Ukrycie rozsyłania ESSID

Namiastka bezpieczeństwa

- Ukrycie rozsyłania ESSID
- Filtracja MAC

Namiastka bezpieczeństwa

- Ukrycie rozsyłania ESSID
- Filtracja MAC
- „Zabawa” adresami IP

Namiastka bezpieczeństwa

- Ukrycie rozsyłania ESSID
- Filtracja MAC
- „Zabawa” adresami IP
- Ograniczenie do minimum mocy nadajnika

WEP

- WEP (ang. *Wired Equivalent Privacy*)

WEP

- WEP (ang. *Wired Equivalent Privacy*)
- Przestarzały standard służący do zapewnienia „prywatności”, przedstawiony w 1997

WEP

- WEP (ang. *Wired Equivalent Privacy*)
- Przestarzały standard służący do zapewnienia „prywatności”, przedstawiony w 1997
- Podatny na ataki kryptoanalityczne

WEP

- WEP (ang. *Wired Equivalent Privacy*)
- Przestarzały standard służący do zapewnienia „prywatności”, przedstawiony w 1997
- Podatny na ataki kryptoanalityczne
- Efekt – ogólnodostępne oprogramowanie i sprzęt łamią zabezpieczenia w kilka(naście) minut

WEP – zasada działania

- Szyfr strumieniowy RC4 do szyfrowania

WEP – zasada działania

- Szyfr strumieniowy RC4 do szyfrowania
- CRC-32 do zapewnienia integralności

WEP – zasada działania

- Szyfr strumieniowy RC4 do szyfrowania
- CRC-32 do zapewnienia integralności
- 128 lub 64 bitowe klucze
  - 24 bitowy IV + 40 bitowy klucz (5 bajtów)
  - 24 bitowy IV + 104 bitowy klucz (13 bajtów)

WEP – zasada działania

- Szyfr strumieniowy RC4 do szyfrowania
- CRC-32 do zapewnienia integralności
- 128 lub 64 bitowe klucze
  - 24 bitowy IV + 40 bitowy klucz (5 bajtów)
  - 24 bitowy IV + 104 bitowy klucz (13 bajtów)
- Rzadko spotykane klucze 256 bitowe

WEP – i po co to wszystko?

- Sierpień 2001 – Scott Fluhrer, Itsik Mantin, Adi Shamir publikują kryptoanalizę WEP, atak oparty o tę metodę nazywamy FMS

WEP – i po co to wszystko?

- Sierpień 2001 – Scott Fluhrer, Itsik Mantin, Adi Shamir publikują kryptoanalizę WEP, atak oparty o tę metodę nazywamy FMS
  - co najmniej 200 000 pakietów – klucz 64-bitowy
  - co najmniej 500 000 pakietów – klucz 128-bitowy

WEP – i po co to wszystko?

- Sierpień 2001 – Scott Fluhrer, Itsik Mantin, Adi Shamir publikują kryptoanalizę WEP, atak oparty o tę metodę nazywamy FMS
  - co najmniej 200 000 pakietów – klucz 64-bitowy
  - co najmniej 500 000 pakietów – klucz 128-bitowy
- 17 ataków KoreK-a.

WEP – i po co to wszystko?

- Sierpień 2001 – Scott Fluhrer, Itsik Mantin, Adi Shamir publikują kryptoanalizę WEP, atak oparty o tę metodę nazywamy FMS
  - co najmniej 200 000 pakietów – klucz 64-bitowy
  - co najmniej 500 000 pakietów – klucz 128-bitowy
- 17 ataków KoreK-a.
- 2007 – Erik Tews, Andrei Pychkine and Ralf-Philipp Weinmann (atak PTW)

WEP – i po co to wszystko?

- Sierpień 2001 – Scott Fluhrer, Itsik Mantin, Adi Shamir publikują kryptoanalizę WEP, atak oparty o tę metodę nazywamy FMS
  - co najmniej 200 000 pakietów – klucz 64-bitowy
  - co najmniej 500 000 pakietów – klucz 128-bitowy
- 17 ataków KoreK-a.
- 2007 – Erik Tews, Andrei Pychkine and Ralf-Philipp Weinmann (atak PTW)
  - 40 000 pakietów – klucz 128-bitowy – 50%
  - 85 000 pakietów – klucz 128-bitowy – 95%

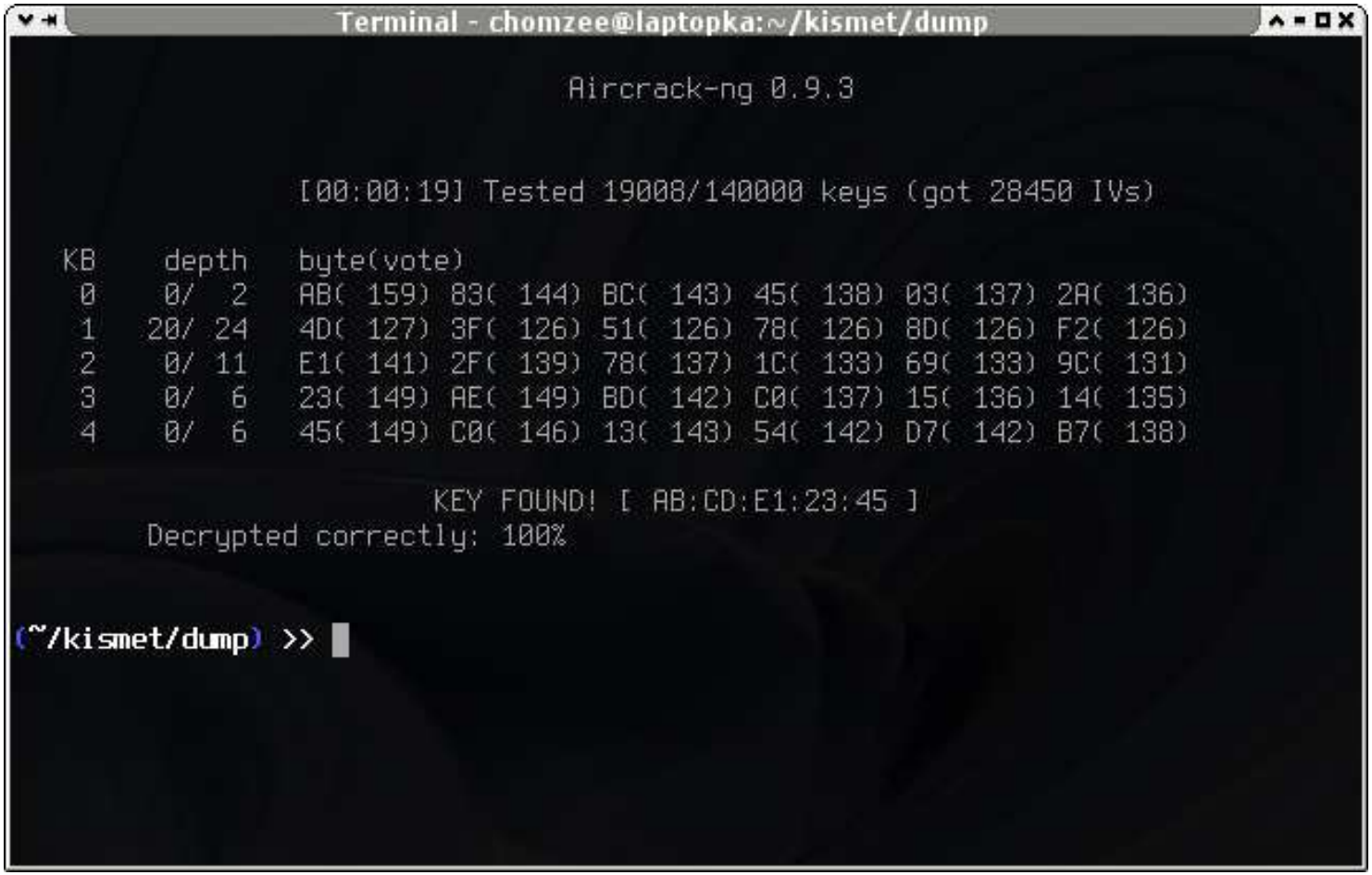
sposób na WEP – jeszcze szybciej!

- Wykorzystanie protokołu ARP do generowania sztucznego ruchu w sieci

sposób na WEP – jeszcze szybciej!

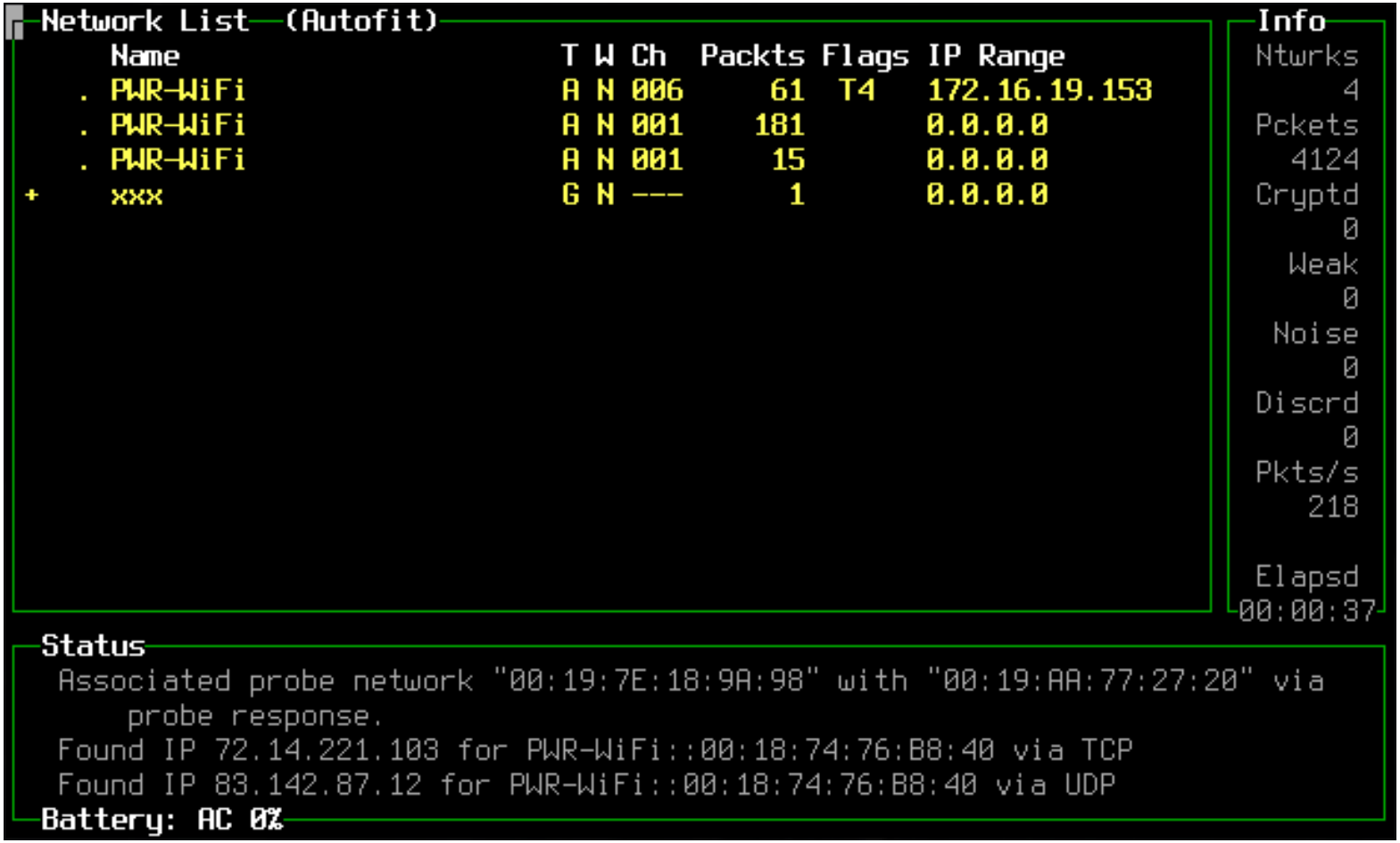
- Wykorzystanie protokołu ARP do generowania sztucznego ruchu w sieci
- **40 000 pakietów w dwie minuty**

WEP pwn3d!



http://aircrack-ng.org/

Kismet również przydatny



http://www.kismetwireless.net/

WPA

- WPA (ang. *WiFi Protected Access*) następca WEP, wprowadzony przez organizację WiFi w kwietniu 2003

WPA

- WPA (ang. *WiFi Protected Access*) następca WEP, wprowadzony przez organizację WiFi w kwietniu 2003
- Standard przejściowy pomiędzy WEP a WPA2, możliwa migracja z WEP bez zmiany sprzętu (konieczna wymiana oprogramowania/firmware)

WPA

- WPA (ang. *WiFi Protected Access*) następca WEP, wprowadzony przez organizację WiFi w kwietniu 2003
- Standard przejściowy pomiędzy WEP a WPA2, możliwa migracja z WEP bez zmiany sprzętu (konieczna wymiana oprogramowania/firmware)
- $$WPA = 802.1x + EAP + TKIP + MIC$$

WPA

- WPA (ang. *WiFi Protected Access*) następca WEP, wprowadzony przez organizację WiFi w kwietniu 2003
- Standard przejściowy pomiędzy WEP a WPA2, możliwa migracja z WEP bez zmiany sprzętu (konieczna wymiana oprogramowania/firmware)
- $$WPA = 802.1x + EAP + TKIP + MIC$$
- Haszowanie IVs, generacja nowych kluczów co 10 000 pakietów

WPA

- WPA (ang. *WiFi Protected Access*) następca WEP, wprowadzony przez organizację WiFi w kwietniu 2003
- Standard przejściowy pomiędzy WEP a WPA2, możliwa migracja z WEP bez zmiany sprzętu (konieczna wymiana oprogramowania/firmware)
- $$WPA = 802.1x + EAP + TKIP + MIC$$
- Haszowanie IVs, generacja nowych kluczów co 10 000 pakietów
- Listopad 2008 – praktyczne ataki kryptoanalityczne przeciwko WPA

WPA2

- WPA2, znany również jako IEEE 802.11i

WPA2

- WPA2, znany również jako IEEE 802.11i
- Zatwierdzony 24 czerwca 2004

WPA2

- WPA2, znany również jako IEEE 802.11i
- Zatwierdzony 24 czerwca 2004
- Szyfr blokowy Rijndael, AES (ang. *Advanced Encryption Standard*)

WPA2

- WPA2, znany również jako IEEE 802.11i
- Zatwierdzony 24 czerwca 2004
- Szyfr blokowy Rijndael, AES (ang. *Advanced Encryption Standard*)
- $$WPA2 = 802.1x + RSN + CCMP$$

Sposób na WPA/WPA2?

- Przechwycić handshake...

Sposób na WPA/WPA2?

- Przechwycić handshake...
- ... po czym pozostaje atak słownikowy

Sposób na WPA/WPA2?

- Przechwycić handshake...
- ... po czym pozostaje atak słownikowy
- Brute force mija się z celem, gdy hasło jest silne

Obrona w wyższych warstwach

- Bardzo wysoki poziom bezpieczeństwa zapewnia oprogramowanie VPN

Obrona w wyższych warstwach

- Bardzo wysoki poziom bezpieczeństwa zapewnia oprogramowanie VPN
- OpenVPN – przenośne, wolne oprogramowanie

Obrona w wyższych warstwach

- Bardzo wysoki poziom bezpieczeństwa zapewnia oprogramowanie VPN
- OpenVPN – przenośne, wolne oprogramowanie
- Wymagany dobrze skonfigurowany firewall (`iptables`)

Pytania?

Bibliografia

- Piotr Metzger, „Anatomia PC”, wydanie IX, Helion 2004
- dr inż. Zbigniew Jóskiewicz, „Systemy telekomunikacji ruchowej 1”, wykład, PWr 2004
- http://dipol.com.pl/
- http://wifi.owe.pl/
- http://www.wi-fiplanet.com/
- http://images.google.com/
- http://en.wikipedia.org/

Dziękuję za uwagę.