Sieci Bezprzewodowe
Część II

Michał Kalewski

Instytut Informatyki
Politechnika Poznańska

$Id: wireless_part2.lyx,v 1.8 2007-12-14 14:49:50 mkalewski Exp $

Plan wykładu

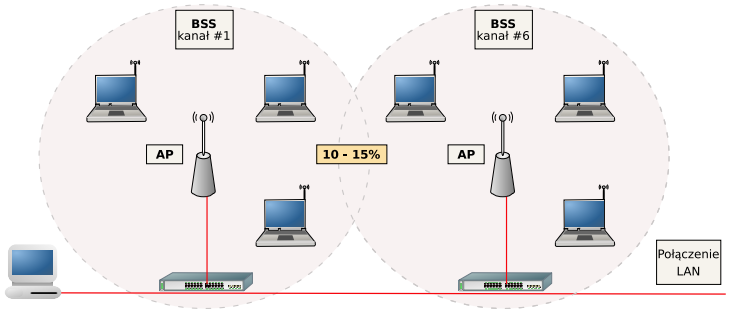
Bezprzewodowe sieci lokalne 802.11* – topologie

Bezprzewodowe Sieci Lokalne 802.11* – topologie

Topologie

- Topologia sieci **IBSS**, *ad-hoc*.
- Topologia sieci **BSS**.
- Topologia sieci **ESS**.
- Topologia sieci z powielaniem **AP** (ang. *wireless repeater topology*).
- Topologia sieci z redundantnym **AP** (ang. *system redundancy topology*) oraz wyrównywanie obciążenia (ang. *load balancing*).
- Roaming w sieciach bezprzewodowych na warstwie 2 (ang. *WLAN roaming*).
- Połączenia mostowe (ang. *bridge connection*).
- Sieci wirtualne **VLAN** (ang. *Virtual Local Area Network*) w ramach sieci bezprzewodowych.

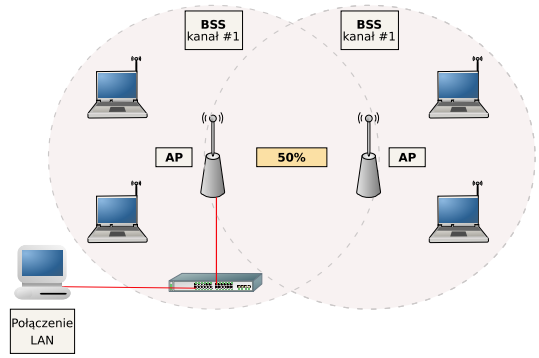
ESS – nakładanie się zasięgów



Extended Basic Service Set

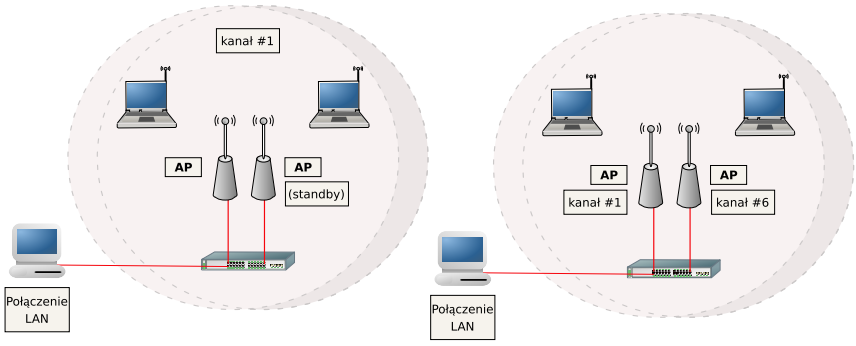
Powielanie AP

Powiększenie zasięgu sieci bezprzewodowej.
Istotnie zmniejsza przepustowość!



Wireless Repeater Topology

Redundancja AP oraz wyrównywanie obciążenia



System Redundancy Topology

Load Balancing

WLAN roaming na warstwie 2 (1)

Przetwarzanie realizowane w sieciach **WLAN** z roaming-iem na warstwie 2:

- **przyłączanie** (ang. *association*) – obejmuje wymianę wiadomość: $association\,request$ i $association\,response$;
- w przypadku wielu odpowiedzi $association\,response$ (od wielu **AP**), **STA** podejmuje decyzje, do którego **AP** się przyłączyć (na podstawie m.in. siły sygnału);
- po przyłączeniu **STA** do **AP** (#1) tworzony jest tzw. identyfikator połączenia (ang. *association ID*) oraz **AP** (#1) zapamiętuje adres **MAC** stacji;

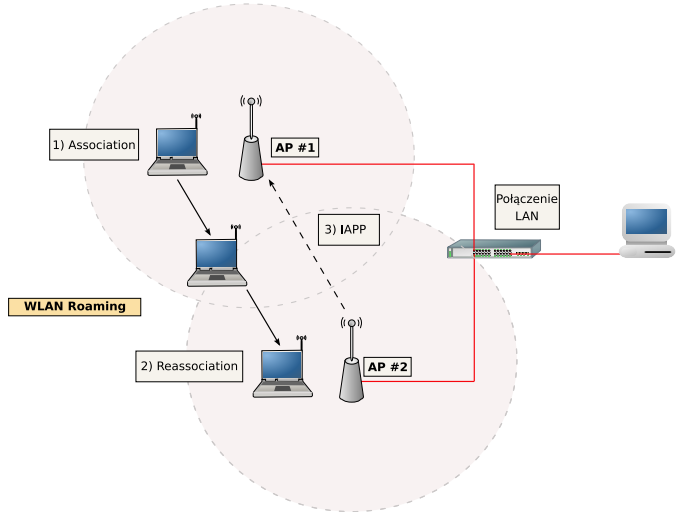
...

WLAN roaming na warstwie 2 (2)

- w przypadku problemów z połączeniem **STA** może zmniejszyć prędkość transmisji lub w ostateczności dokonać wyboru (z wykorzystaniem skanowania) innego **AP** (z lepszą jakością połączenia);
  802.11b: 1 / 2 / 5,5 / 11 Mb/s; **802.11ag**: 6 / 9 / 12 / 18 / 24 / 36 / 48 / 54 Mb/s.
- **przełączenie** (ang. *reassociation*) – obejmuje wymianę wiadomości: $reassociation\ request$ i $reassociation\ response$;
- **AP** (#2), do którego przełączyła się **STA**, tworzy nowy identyfikator połączenia oraz zapamiętuje adres **MAC** stacji;
- **AP** (#2) informuje **AP** (#1) o przełączeniu **STA** z wykorzystaniem protokołu **IAPP** (ang. *Inter-Access Point Protocol*) opisanego w **802.11f**. ■

Uwaga: na całej drodze **STA** korzysta ze stałego adresu **IP** w ramach tej samej **sieci IP**; zmiana **sieci IP** wymaga roaming-u na warstwie 3.

WLAN roaming na warstwie 2 – przykład



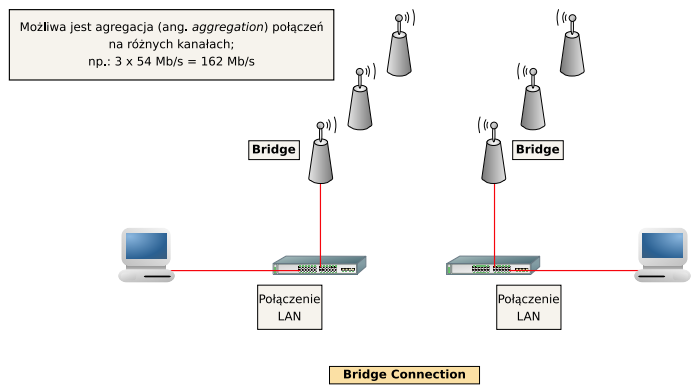
Połączenia mostowe

Bezprzewodowe mosty (ang. *wireless bridges*) służą do łączenia dwóch lub więcej przewodowych sieci lokalnych **LAN** – standard **802.11c**.

Połączenia na odległość nawet kilku kilometrów – w zależności od stosowanych anten.

Bezprzewodowe mosty mogą funkcjonować w różnych trybach: *root bridge*, *non-root bridge with clients*, *non-root bridge without clients*.

Połączenia mostowe – przykład



Tryby mostów bezprzewodowych

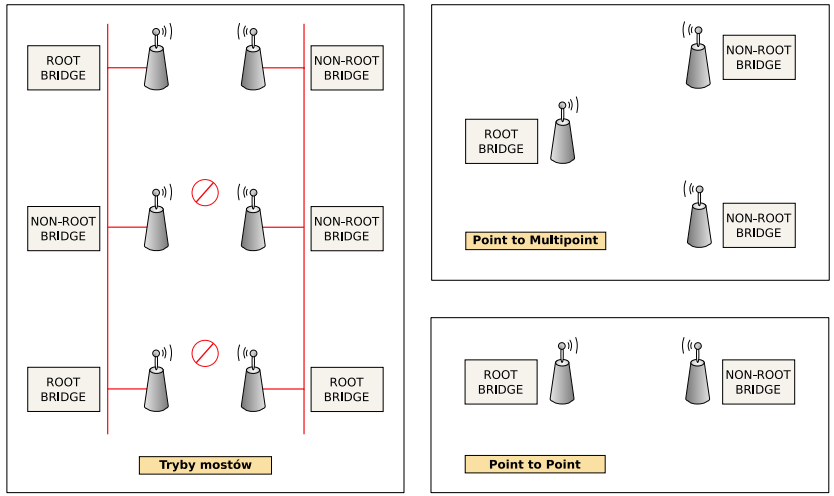
Root bridge:

- akceptuje połączenia i komunikacje tylko z urządzeniami w trybie *non-root bridge*;
- nie pozwala na komunikacje z innymi mostami w trybie *root bridge*;
- może łączyć się z jednym (ang. *point to point*) lub wieloma (ang. *point to multipoint*) mostami *non-root bridge*.

Non-root bridge:

- akceptuje połączenia i komunikuje się z mostami w trybie *root bridge*;
- nie pozwala na (bezpośrednią) komunikacje z innymi mostami w trybie *non-root bridge*;
- może obsługiwać połączenia od **STA** – w trybie *non-root bridge with clients*.

Tryby mostów bezprzewodowych – przykłady



Sieci VLAN w ramach sieci bezprzewodowych (1)

W sieciach bezprzewodowych istnieje możliwość konfigurowania sieci wirtualnych **VLAN** (ang. *Virtual Local Area Network*) oraz łączenia ich z sieciami przewodowymi za pomocą standardu **802.1Q**.

Sieci **VLAN** w sieciach radiowych realizowane są poprzez przypisanie (w ramach jednego **AP**) różnych identyfikatorów **SSID** oraz różnych kluczy szyfrowania **WEP**.

W konsekwencji tylko stacje należące do określonej sieci **VLAN** mogą odbierać ramki z tej sieci wirtualnej – mówi się wówczas o tzw. segregacji ruchu w sieci radiowej (ang. *traffic segregation*).

Zalety stosowania sieci **VLAN** to m.in.: segmentacja sieci (ang. *segmentation*), bezpieczeństwo (ang. *security*) oraz kontrola rozgłaszania (ang. *broadcast control*).

Sieci VLAN w ramach sieci bezprzewodowych (2)

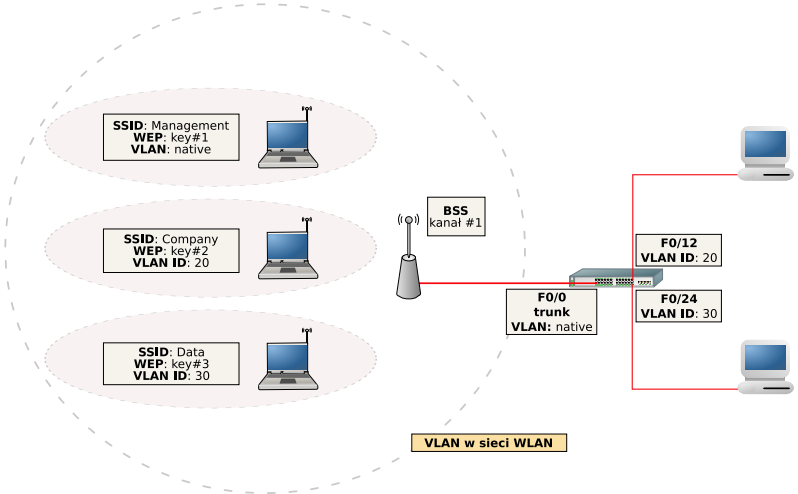
Sieci **VLAN** w ramach sieci bezprzewodowych oznaczane są także za pomocą identyfikatorów $VLAN\ ID$.

VLAN native to sieć, w której transmitowane ramki nie posiadają identyfikatorów $VLAN\ ID$ (ang. *untagged frames*).

Ramki, które nie posiadają identyfikatorów sieci wirtualnej, a które docierają do **AP** poprzez port **trunk** (**802.1Q**) są przekazywane do sieci **VLAN native**.

Ramki, które docierają do **AP** z sieci **VLAN native** są dalej przesyłane bez identyfikatora sieci wirtualnej.

Sieci VLAN – przykład



Elementy bezpieczeństwa w sieciach 802.11*

Elementy bezpieczeństwa w sieciach 802.11*

WEP

WEP (ang. *Wired Equivalent Privacy*) – protokół bezpieczeństwa warstwy łącza danych sieci bezprzewodowych 802.11*.

WEP wymaga aby komunikujące się strony posiadały własne (identyczne) **klucze tajne**.

Szyfrowanie (**strumieniowe**) w **WEP** odbywa się z zastosowaniem algorytmu **RC4** (twórcą algorytmu jest **Ronald Rivest**).

RC4 generuje **strumień szyfrujący**, z którymi następnie różnicowana (operacją **XOR**) jest zawartość jawnych danych.

WEP – klucze

Klucze tajne WEP mogą mieć następujące długości:

- **40 bitów**: (5 znaków **ASCII** lub 10 cyfr **HEX**) + 24 bity IV = 64 bity;
- **104 bity**: (13 znaków **ASCII** lub 26 cyfr **HEX**) + 24 bity IV = 128 bitów.

Informacje o 64 i 128 bitowych kluczach obejmują także generowane tzw. **wektory inicjujące** IV (ang. *Initialization Vector*) i w praktyce odnoszą się do kluczy tajnych 40 i 104 bitowych.

Faktycznie dłuższe klucze tajne występują w rozwiązaniach firmowych oraz w **WPA**/**WPA2**.

WEP – etapy (1)

Szyfrowanie ramki danych DF z wykorzystaniem protokołu **WEP** składa się z następujących etapów:

- na koniec ramki dodawana jest suma kontrolna ICV (ang. *Integrity Check Value*) jawnej zawartości ramki wyznaczana przy pomocy algorytmu **CRC-32,**
  - uzyskujemy: $DF = DF.ICV(DF)$;
- generator liczb pseudolosowych wyznacza 24-bitowy wektor inicjujący IV (ang. *Initialization Vector*);
- do wektora IV dołączany jest klucz tajny szyfrowania K,
  - uzyskujemy: $IV.K$;

...

WEP – etapy (2)

- wektor $IV.K$ jest szyfrowany algorytmem strumieniowym **RC4,**
  - uzyskujemy pseudolosową sekwencję $RC4(IV.K)$ – strumień szyfrujący;
- wykonywana jest funkcja logiczna **XOR** (oznaczona $\oplus$) na zaszyfrowanym wektorze $RC4(IV.K)$ i jawnej ramce DF,
  - uzyskujemy zaszyfrowaną ramkę $CDF = (DF.ICV(DF) \oplus RC4(IV.K))$;
- wektor IV jest dodawany na początku zaszyfrowanej ramki CDF w postaci jawnej;
- ostatecznie uzyskujemy ramkę: $IV.CDF$. ■

WEP – deszyfrowanie

Deszyfrowanie ramki $IV.CDF$ wymaga następujących etapów:

- na podstawie IV z ramki oraz klucza tajnego K tworzony jest wektor $IV.K$;
- wektor $IV.K$ jest szyfrowany algorytmem strumieniowym **RC4**,
  - uzyskujemy sekwencję $RC4(IV.K)$ – identyczną jak przy szyfrowaniu;
- wykonywana jest funkcja logiczna **XOR** na zaszyfrowanym wektorze $RC4(IV.K)$ i ramce CDF;
  - uzyskujemy $DF.ICV(DF) = (CDF \oplus RC4(IV.K))$;
- obliczana jest suma kontrolna uzyskanej ramki DF, która jest porównywana z $ICV(DF)$. ■

Algorytm RC4

RC4 (ang. *Rivest Cipher 4*) generuje pseudolosowy strumień bitów (ang. *pseudorandom keystream*), który jest używany do szyfrowania danych jawnych z wykorzystaniem różnicowania (**XOR**).

RC4 wykonywany jest w dwóch etapach:

1. **procedura inicjacji klucza KSA** (ang. *Key-Scheduling Algorithm*) – tworzy początkową permutację liczb;
2. **algorytm pseudolosowej generacji PRGA** (ang. *Pseudo-Random Generation Algorithm*) – generuje właściwą liczbę bajtów strumienia szyfrującego.

Algorytm RC4 – KSA

Procedura inicjacji klucza **KSA** realizowana jest przez następujący algorytm:

1: **KSA** (K)**:**
2: $dk \leftarrow rozmiar\_tablicy\ K$;
3: $S[256]$;
4: $j := 0$;
5: **for** $i = 0$ **to** 255 **do**
6: $S[i] := i$;
7: **endfor**
8: **for** $i = 0$ **to** 255 **do**
9: $j := (j + S[i] + K[i \bmod dk]) \bmod 256$;
10: zamien($S[i]$, $S[j]$);
11: **endfor**

■

Tablica K składa się z pseudolosowego ciągu wektora inicjującego oraz z klucza tajnego.

Algorytm RC4 – PRGA

Pseudolosowa generacja **PRGA** wykonywana jest zgodnie z następującym algorytmem:

1: **PRGA** (S)**:** //tablica S pochodzi z procedury **KSA**
2: $i := 0$;
3: $j := 0$;
4: **petla generacji strumienia:**
5: $i := (i + 1) \bmod 256$;
6: $j := (j + S[i]) \bmod 256$;
7: zamien($S[i]$, $S[j]$);
8: $z := S[S[i] + S[j]]$;
9: **wynik**: z xor $dane$;

■

WEP – problemy

- Klucz tajny jest najczęściej jednakowy dla wszystkich użytkowników, co oznacza, że mogą oni się wzajemnie podsłuchiwać.
- Wektor IV w praktyce bywa powtarzany dla wielu (kolejnych) ramek, co umożliwia tzw. *atak powtórzonego klucza*.
- 24 bitowy wektor IV musi się powtarzać co $2^{24} \cong 16,7\,mln$ pakietów – w praktyce oznacza to, że jest on powtarzany co kilkadziesiąt minut (w najgorszym przypadku po kilku godzinach).

Znane ataki, mi.in:

- Borisov N., Goldberg I., Wgner D., **Intercepting Mobile Communication: The Insecurity of 802.11**, 17th International Conference on Mobile Computing and Networking, ACM, str.: 180-188, 2001.
- Fluhrer S.,R., Mantin I., Shamir A., **Weaknesses in the Key Scheduling Algorithm of RC4**, Selected Areas in Cryptography, str.: 1-24, 2001.

WEP – atak powtórzonego klucza

Atak powtórzonego klucza:

P_1 – szyfrogram danych P_0 za pomocą klucza K, czyli: $P_1 = (P_0 \oplus K)$.

Q_1 – szyfrogram danych Q_0 za pomocą (tego samego co wyżej) klucza K, czyli: $Q_1 = (Q_0 \oplus K)$.

Można wówczas wyeliminować klucz K:
$S_1 = (P_0 \oplus K) \oplus (Q_0 \oplus K) = P_0 \oplus Q_0 \oplus K \oplus K = P_0 \oplus Q_0 \oplus 0 = P_0 \oplus Q_0$.

Jeśli jeden z tekstów P_0 lub Q_0 jest znany, to odszyfrowanie drugiego jest natychmiastowe.

($\oplus$ – operacja różnicowania **XOR**)

WEP – atak FMS (1)

Atak FMS (Fluhrer, Mantin, Shamir) opiera na kilku obserwacjach, m.in.:

- istnieją tzw. **słabe wektory** IV (ang. *weak key*), które inicjują zbyt prostą permutację początkową,
  mają one postać $(B + 3, 255, X)$, gdzie B to numer bajtu klucza, który ma być złamany, a X to dowolna wartość – np.: 3, 255, 7;
- w szyfrowanych ramkach pierwszy bajt ma najczęściej wartość 0xAA$_{hex}$;
- złożoność algorytmu odtwarzania klucza rośnie liniowo ze względu na długość tego klucza.

WEP – atak FMS (2)

Atak FMS jest realizowany w następujący sposób:

- zbierane są duże ilości ramek z wektorami IV;
- za pomocą systematycznej analizy słabych wektorów IV odtwarzany jest tajny klucz;
  - każdy słaby wektor wykorzystywany jest do złamania innej części klucza, zgodnie ze wzorem $(B + 3, 255, X)$. ■

W praktyce **atak FMS** wymaga przechwycenia około miliona wektorów IV (dla klucza o długości 104/128 bitów).

WEP – przykład łamania za pomocą pakietu `aircrack-ng`

`aircrack-ng` to zestaw darmowych programów służących do łamania kluczy **WEP** i **WPA-PSK**.

Internet: http://www.aircrack-ng.org/

Przykład: łamanie klucza WEP

1. `# iwconfig ath0 mode monitor`
   ustawienie karty bezprzewodowej w tryb nasłuchiwania ramek (ang. *promiscuous mode*)
2. `# airodump-ng --channel 3 --bssid 00:16:9C:92:8E:80 --write output ath0`
   zapis odbieranych ramek: na wskazanym kanale, dla wskazanego punktu dostępowego i do pliku o podanej nazwie
3. `# aireplay-ng -b 00:16:9C:92:8E:80 -h 12-F0-57-BC-84-38 -x 600 --arpreplay ath0`
   generowanie zapytań **ARP** do punktu dostępowego (600 zapytań na sekundę)
4. `# aircrack-ng -z output*.cap`
   uruchomienie procedury poszukiwania klucza w oparciu o zapisane w pliku ramki

Zalecenia bezpieczeństwa w sieciach 802.11*

Podstawowe zalecenia bezpieczeństwa w sieciach **802.11***:

- wyłączyć rozgłaszanie **SSID** w **AP**;
- zmienić domyślne ustawienia w **AP** (SSID, adresy IP, hasła itp.) **!**;
- włączyć szyfrowanie (z kluczem 104/128 bitowym);
- używać losowych kluczy **WEP** (trudnych do odgadnięcia);
- wprowadzać częste zmiany kluczy **WEP**;
- stosować sieci wirtualne **VLAN**;
- wprowadzić filtracje adresów **MAC** i/lub adresów **IP**;
- jeśli to możliwe używać systemów **WPA**/**WPA2;**
- ostatecznie zastosować **VPN** (ang. *Virtual Private Network*).

Przykład: generowanie pseudolosowego klucza WEP

```
$ dd if=/dev/random bs=1 count=26 2>/dev/null | xxd -ps
```

WPA

WPA (ang. *WiFi Protected Access*) – system zabezpieczeń dla sieci bezprzewodowych 802.11*, oryginalnie wprowadzony przez **Wi-Fi Aliance.**

WPA stosuje część zaleceń standardu **802.11i**. **WPA2** obejmuje pełne zalecenia tego standardu – m.in. zastąpienie algorytmu **RC4** szyfrowaniem **AES** (ang. *Advanced Encryption Standard*).

WPA – tryby pracy

Dwa tryby pracy **WPA**:

1. **WPA-PSK** (ang. *Pre-Shared Key* lub *Personal*) – dla zastosowań domowych i w niewielkich biurach; działa w oparciu o *hasła użytkowników* (ang. *passphrase*);
2. **WPA-Enterprise** – wykorzystuje protokół **EAP** (ang. *Extensible Authentication Protocol*) – opisany w **RFC** 3748 – który obejmuje metody uwierzytelniania w architekturze klient serwer (tzw. serwer *Radius*).

802.11i – nawiązanie bezpiecznego kontekstu komunikacji (1)

Nawiązanie bezpiecznego kontekstu komunikacji składa się z czterech faz:

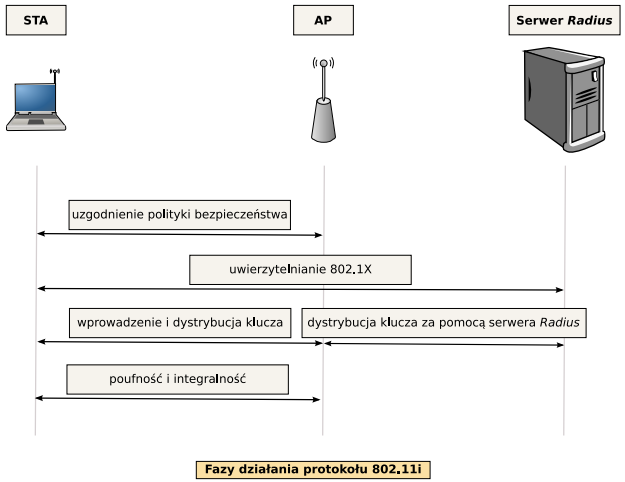
1. **Uzgadnianie polityki bezpieczeństwa** – m.in.:
   - metody uwierzytelniania, np.: **PSK** (ang. *Pre-Shared Key*), **802.1X**;
   - protokół bezpieczeństwa dla transmisji pojedynczej, np.: **TKIP** (ang. *Temporal Key Integrity Protocol*) – protokół dynamicznego zarządzania kluczami w oparciu o mechanizmy **WEP**.
2. **Uwierzytelnienie 802.1X** – uwierzytelnienie wykorzystujące protokół **EAP**.

...

802.11i – nawiązanie bezpiecznego kontekstu komunikacji (2)

3. **Generowanie i dystrybucja klucza** – klucze posiadają ograniczony czas ważności (np. dla **TKIP** – co 10 000 pakietów).
4. **Zapewnianie integralności i poufności danych** – integralność danych: algorytm *Michael* (podsumowanie ramki funkcją skrótu).

801.11i – fazy działania



Fazy działania protokołu 802.11i

Szerokopasmowe łącza bezprzewodowe 802.16

Szerokopasmowe łącza bezprzewodowe 802.16

Sieci 802.16

Szerokopasmowe łącza bezprzewodowe są realizowane w oparciu o standard **802.16** – **Interfejs radiowy dla stacjonarnych szerokopasmowych systemów dostępu bezprzewodowego** (ang. *Air interface for fixed broadband wireless access systems*).

Sieci te bywają także nazywane **Wireless MAN** (**WMAN**) lub **WiMax**.

Rok publikacji standardu: 2001.

Różnice oczekiwań pomiędzy 802.11 i 802.16

Sieci **802.16** dedykowane są dla innych zastosowań niż sieci **802.11**, oto podstawowe różnice:

- Sieci **802.11** wspierają mobilność użytkowników, podczas gdy sieci **802.16** są raczej dedykowane dla połączeń pomiędzy budynkami.
- Sieci **802.16** umożliwiają komunikację pełno-dupleksową – w sieciach **802.11** interfejsy radiowe są raczej pół-dupleksowe.
- Sieci **802.16** mogą obejmować rozległe obszary, a więc moc sygnału może się istotnie różnić w zależności od odległości od stacji bazowej.
- Bezpieczeństwo w sieciach **802.16** ze względu na ich zasięg jest niezbędne.
- Sieci **802.16** wymagają istotniejszego wsparcia dla jakości usług **QoS** (ang. *Quality of Service*).

Warstwa fizyczna sieci 802.16 (1)

Sieci **802.16** w funkcjonują w paśmie od 10 do 66 GHz.

Stosowane są trzy metody modulacji:

1. **64-QAM** (ang. *64-level Quadrature Amplitude Modulation*) – 6 bitów na bod, co przekłada się na przepustowość 150 Mb/s (tylko dla najbliższych połączeń);
2. **16-QAM** (ang. *16-level Quadrature Amplitude Modulation*) – 4 bity na bod, co przekłada się na przepustowość 100 Mb/s (dla połączeń o średniej odległości);
3. **QPSK** (ang. *Quadrature Phase Shift Keying*) – 2 bity na bod, co przekłada się na przepustowość 50 Mb/s (dla najbardziej oddalonych połączeń).

Warstwa fizyczna sieci 802.16 (2)

Przydział pasma realizowany jest z wykorzystaniem dwóch technik:

1. **FDD** (ang. *Frequency Division Duplexing*) – praca dwukierunkowa z podziałem częstotliwości;
2. **TDD** (ang. *Time Division Duplexing*) – praca dwukierunkowa z podziałem czasu.

Pojedyncza fizyczna transmisja może obejmować wiele ramek **MAC** – pozwala to na redukcję ilości preambuł i nagłówków warstwy fizycznej.

Ze względu na ilość możliwych zakłóceń, a co za tym idzie błędów transmisji, korekcja błędów jest przeprowadzana w warstwie fizycznej.

Podwarstwy MAC sieci 802.16

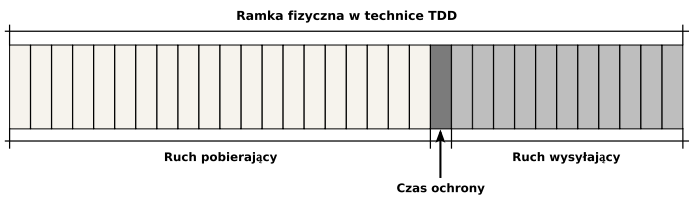
W przypadku **TDD** każda ramka warstwy fizycznej podzielona jest na szczeliny – osobne dla **ruchu pobierającego** (ang. *downstream*) oraz osobne dla **ruchu wysyłającego** (ang. *upstream*).

Połączenie w sieci 802.16 jest realizowane z wykorzystaniem uwierzytelniania poprzez **RSA** (Rivest, Shamir Adleman) oraz certyfikaty **X509**. Dane ramek są szyfrowane algorytmem **DES** (ang. *Data Encryption Standard*) z kluczem symetrycznym.

Ruch pobierający jest mapowany na szczeliny czasowe przez stacje bazową, a przydział do kanału wysyłającego jest uzależniony od wybranej **klasy usług**.

TDD – przykład ramki

FDD (ang. *Frequency Division Duplexing*) -- praca dwukierunkowa z podziałem częstotliwości.
TDD (ang. *Time Division Duplexing*) -- praca dwukierunkowa z podziałem czasu.



Ramka i szczeliny czasowe w pracy dwukierunkowej z podziałem czasu

Klasy usług sieci 802.16

Zdefiniowane są cztery **klasy usług**, które determinują sposób przydziału kanału wysyłającego:

1. **usługa ze stałą szybkością transmisji** – dedykowana dla transmisji nieskompresowanego głosu;
2. **usługa ze zmienną szybkością transmisji w czasie rzeczywistym** – dedykowane kompresowanych transmisji mediów oraz innych niekrytycznych aplikacji czasu rzeczywistego;
3. **usługa ze zmienną szybkością transmisji nie w czasie rzeczywistym** – dedykowana dla intensywnych transmisji, które nie wymagają czasu rzeczywistego (np. transmisja plików);
4. **usługa z użyciem dostępnych możliwości** – dla wszystkich pozostałych sytuacji; w tym wypadku stacja musi rywalizować z innymi stacjami o dostęp do kanału.

Sieci Bluetooth – 802.15.1

Sieci Bluetooth – 802.15.1

Sieci Bluetooth

Pierwsze opracowanie (v1.0) sieci **Bluetooth** zostało wykonane przez firmy Ericsson, IBM, Intel, Nokia i Toshiba w 1999 r.

Odpowiedni standard IEEE nosi numer **802.15.1** – wzorowany na specyfikacji v1.1.

Bluetooth działa w paśmie 2,4 GHz **ISM** (**zakłóca 802.11b/g !**), dzieląc je na 79 pod-kanałów o szerokości 1MHz – wykorzystuje się technikę skokowej zmiany kanału.

Pozwala to na realizację następujących przepustowości:

- **v1.1**, **v1.2**: 723,1 kb/s;
- **v2.0**: 2,1 Mb/s.

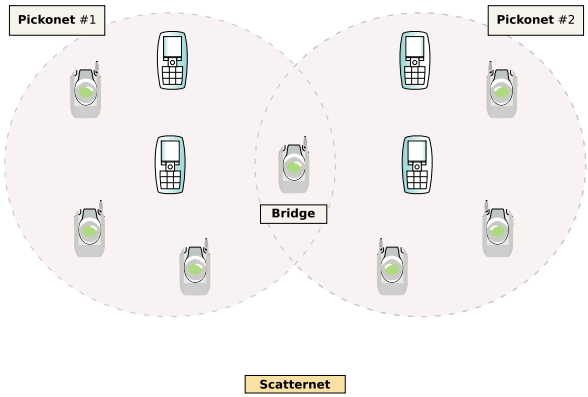
Architektura sieci Bluetooth (1)

Podstawową jednostką sieci **Bluetooth** jest tzw. **pikosieć** (ang. *pikonet*), która składa się z **węzła głównego** (ang. *master node*) oraz maksymalnie siedmiu **węzłów podrzędnych** (ang. *slave node*) w odległości do 10 m.

Pikosieci mogą być ze sobą połączone za pomocą węzłów nazywanych **mostami** (ang. *bridge node*) tworząc tzw. **sieci rozrzucone** (ang. *scatternet*).

W pikosieci oprócz węzłów podrzednych może być maksymalnie do 255 węzłów, które są w stanie niskiego poboru mocy i które jedynie oczekują na sygnał aktywacji.

Architektura sieci Bluetooth (2)



Zastosowania sieci Bluetooth (1)

Specyfikacja **Bluetooth** wymienia 13 konkretnych zastosowań tych sieci, są one zwane **profilami** (ang. *profiles*):

- **dostęp ogólny** (ang. *generic access*) – procedury zarządzania łączem, tj. nawiązanie i utrzymanie bezpiecznych kanałów pomiędzy węzłami (wymagany);
- **wykrywanie usług** (ang. *service discovery*) – wykrywanie usług innych urządzeń (wymagany);
- **port szeregowy** (ang. *serial port*) – protokół transportowy i emulacja lini szeregowej;
- **ogólna wymiana obiektów** (ang. *generic object exchange*) – relacje klient-serwer dla wymiany obiektów (każdy węzeł może być zarówno klientem jak i serwerem);
- **dostęp do sieci lokalnej** (ang. *LAN access*) – protokół dostępu do sieci stacjonarnej z urządzenia **Bluetooth** (analogia do 802.11);

...

Zastosowania sieci Bluetooth (2)

- **łącza telefoniczne** (ang. *dial-up networking*) – łączenie się komputera poprzez telefon komórkowy z wbudowanym modemem;
- **fax** – wysyłanie i odbieranie faksów z urządzeń **Bluetooth**;
- **telefonia bezprzewodowa** (ang. *cardless telephony*) – połączenia zestawów słuchawkowych ze stacją bazową;
- **intercom** – połączenie dwóch telefonów;
- **zestaw słuchawkowy** (ang. *headset*) – obsługa zestawów słuchwkowych;
- **przekazywanie obiektów** (ang. *object push*) – sposób wymiany prostych obiektów;
- **transfer plików** (ang. *file transfer*);
- **synchronizacja** (ang. *synchronization*) – synchronizacja urządzenia PDA (ang. *Personal Digital Assistant*) z komputerem.

Literatura

Arbaugh W.A., Edney J., **Real 802.11 Security: Wi-Fi Protected Access and 802.11i**, Addison Wesley, 2004.

Gast M. S., **802.11 Wireless Networks: The Definitive Guide**, O'Reilly, 2005.

Lin Y.-B., Pang A.-Ch., **Wireless and Mobile All-IP Networks**, Wiley, 2005.

Roshan P., Leary J., **Wireless Local-Area Network Fundamentals**, Cisco Press, 2003.

Stallings W., **Wireless Communications and Networks**, Pearson Prentice Hall, 2002.

Tanenbaum A. S., **Computer Networks**, Pearson Education Inc., 2003.

Prezentacja jest dostępna w Internecie na stronie:

http://www.cs.put.poznan.pl/mkalewski WWW

pod adresem:

http://www.cs.put.poznan.pl/mkalewski/files/wireless_part2.pdf PDF