Instrukcja laboratoryjna

„Sieci bezprzewodowe IEEE 802.11b/g”

1 Wstęp

Poniższy dokument stanowi instrukcję do ćwiczenia laboratoryjnego zatytułowanego „Sieci bezprzewodowe IEEE 802.11”. Zawiera on opis poszczególnych zadań do wykonania wchodzących w skład ćwiczenia, a także materiał pomocniczy, którego znajomość może ułatwić wykonanie ćwiczenia.

1.1 Cel laboratorium

Celem laboratorium jest uzyskanie przez studentów praktycznej wiedzy z zakresu konfiguracji sieci bezprzewodowych standardu IEEE 802.11. Zadania są zaplanowane w taki sposób, aby umożliwić:

- zapoznanie studentów z konfiguracją bezprzewodowych kart sieciowych w systemach MS Windows i Linux
- zapoznanie studentów z konfiguracją bezprzewodowych punktów dostępowych
- badanie wydajności sieci bezprzewodowych
- lepsze zrozumienie działania protokołów sieciowych
- rozszerzenie umiejętności konfiguracji urządzeń sieciowych pod systemem Linux

1.2 Wymagania stawiane studentom

Laboratorium zostało zaprojektowane tak, aby student mógł się możliwie jak najwięcej nauczyć. Potrzebna jest jednak pewna wiedza niezbędna do sprawnego wykonania ćwiczenia.
Od studentów uczestniczących w laboratorium będzie wymagana:

- dokładna znajomość instrukcji laboratoryjnej
- podstawowa znajomość zagadnień sieciowych

1.3 Przykładowe pytania na wejściówkę

- Tryb ad-hoc sieci bezprzewodowej umożliwia
- Tryb infrastructure sieci bezprzewodowej umożliwia
- Tryb bridge sieci bezprzewodowej umożliwia
- SSID to
- Proces przyłączania do sieci bezprzewodowej rozpoczyna ramka
- Ramka (tutaj nazwa ramki 802.11 - różne nazwy, różne pytania) należy do grupy ramek
- Proces skanowania w trybie "infrastructure" polega na
- W standardzie 802.11g w paśmie 2.4 GHz szybkości transmisji to

- W standardzie 802.11b w paśmie 2.4 GHz szybkości transmisji to
- W standardzie 802.11 b/g (Europa) w paśmie 2.4 GHz zdefiniowano liczbę kanałów równą
- WEP to
- Trybem pracy charakterystycznym tylko dla kart bezprzewodowych jest

1.4 Materiały

1. Instrukcja do ćwiczenia
2. Załącznik do ćwiczenia zatytułowany „Iproute2 i Wireless Tools”
3. Manual do punktu dostępowego DWL900AP+ (DWL2000) - wybrane punkty

Dodatkowe:

4. „Bezpieczeństwo sieci 802.11” Matthew S. Gast, wyd. O’Reilly
5. „100 Sposobów na sieci bezprzewodowe” Rob Flickenger, wyd. O’Reilly
6. „Sieci LAN, MAN, WAN- protokoły komunikacyjne” Józef Woźniak, Krzysztof Nowicki
7. „Przewodowe i bezprzewodowe sieci LAN” Krzysztof Nowicki, Józef Woźniak

2 Struktura laboratorium

2.1 Struktura logiczna

Ćwiczenie będzie przeprowadzone na komputerach wyposażonych w bezprzewodowe karty sieciowe, pracujących pod systemami MS Windows XP i GNU/Linux Debian.

Praca będzie przebiegała w grupach czteroosobowych. Niezwykle istotną sprawą jest współpraca wewnątrz grupy. Ze względu na charakter ćwiczenia, podczas niektórych zadań, fizycznie pracować będzie przy komputerze tylko jedna osoba. Bardzo ważne jest, aby pozostali uczestnicy grupy włączali się w tym czasie czynnie w pracę i obserwowali wyniki.

Na każdą grupę przypada jeden punkt dostępowy D-Link DWL900AP+ albo D-Link DWL2000AP.

2.2 Adresy urządzeń

Adresy numery kanałów i identyfikatory bezprzewodowych punktów dostępowych oraz adresy, które trzeba przypisać bezprzewodowym kartom sieciowym zostaną podane każdej grupie przez prowadzącego podczas zajęć.

3 Zadania laboratoryjne

3.1 Zadanie 1 – Wstępna konfiguracja urządzeń w SO Linux

W zadaniu 1 należy skonfigurować urządzenia bezprzewodowe, aby możliwe było przeprowadzenie następnych zadań . Konfiguracja została podana w poniżej tabeli. W celu pomocy, zostały podane kolejne kroki, które doprowadzą do zadanej konfiguracji.

1. Uruchomić komputer. W menu startowym należy wybrać system Linux. Zalogować się na konto root z hasłem podanym przez prowadzącego.
2. Sprawdzić ustawienia interfejsów sieciowych i w razie potrzeby je skorygować. Na s1 powinien być uruchomiony interfejs eth0, natomiast na s2 – s4 wszystkie interfejsy sieciowe powinny być wyłączone, gdyż nie będą używane.
3. Podłączyć s1 do punktu dostępowego przy pomocy kabla. Kabel jest podłączony do interfejsu eth0. Punkty dostępowe są zresetowane do ustawień fabrycznych.
4. Na s1 zaadresować interfejs eth0 tak, aby możliwa była przez niego komunikacja z punktem dostępowym. Domyślne ustawienia dla punktów dostępowych wyglądają następująco:

urządzenie	nr IP	login	hasło
D-Link	192.168.0.50/24	admin	-
Cisco	10.0.0.1/8	-	-

5. Na s1 uruchomić tryb graficzny poleceniem *startx.* Wejść na stronę konfiguracyjną AP.
   Ustawić identyfikator sieci SSID na ‘apx-yz’, gdzie w miejsce x stawiamy nr grupy, w miejsce y ‘cisco’ lub ‘dlink’ w zależności od tego jaki AP używamy, natomiast w miejsce z wstawiamy nr AP, który jest napisany czerwonym pisakiem na spodzie AP.
   Przykładowa nazwa: **ap2-cisco3.**
   Ustawić kanał na podany przez prowadzącego.
   Ustawić adres IP na podany przez prowadzącego.

Uwaga: Po zmianie adresu IP i zaakceptowaniu zmian nie będzie możliwe dalsze konfigurowanie AP, przez interfejs eth0. Dlaczego?

6. Podłączyć się do odpowiednich punktów dostępowych przy użyciu komendy *iwconfig* z odpowiednimi parametrami.

Wskazówka: Prawdopodobnie ze względu na niedopracowaną wersję sterowników, czasami karty mogą się nie skojarzyć z punktem dostępowym. Aby uniknąć problemów, należy skontrolować czy karta rzeczywiście się połączyła. W tym celu wydajemy komendę *iwconfig* bez parametrów, która wyświetla bieżącą konfigurację interfejsów bezprzewodowych. O właściwym skojarzeniu karty z AP wskazuje adres, przy polu Access Point, inny niż 00:00:00:00:00:00. W razie problemów z podłączeniem, należy poleceniem *start_net* przywrócić domyślne ustawienia karty i spróbować podłączyć się jeszcze raz.

7. Zaadresować interfejs wlan0. Sprawdzić łączność miedzy wszystkimi komputerami w grupie przy pomocy komendy *ping*. **Powiadomić prowadzącego.**

3.2 Szczegółowe zadania

3.2.1 Konfiguracja do pracy w trybie ad-hoc w SO MS Windows

Dla ułatwienia realizacji ćwiczenia wyłączamy zasilanie punktu dostępowego.

3.2.2 Konfiguracja do pracy z punktem dostępowym w SO MS Windows

3.2.3 Konfiguracja do pracy w trybie ad-hoc w SO Linux

3.2.4 Konfiguracja do pracy z punktem dostępowym w SO MS Linux

3.2.5 Badanie wydajności sieci bezprzewodowych w trybie ad-hoc i w trybie infrastructure

3.2.6 Badanie wpływu szyfrowania transmisji WEP na wydajność

3.2.7 Badanie wpływu pracy dwóch sieci na sąsiednich kanałach na wydajność sieci bezprzewodowej

4 Materiał pomocniczy do ćwiczenia

4.1 Ramki w sieciach standardu IEEE 802

4.1.1 Ramka Ethernet

Struktura ramki występującej w sieci LAN standardu IEEE 802.3 została przedstawiona na Rysunku 4-1.

	Preambuła	Start Ramki	Adres Docelowy	Adres Źródłowy	Długość	Dane	Rozszerzenie	Suma Kontrolna
Liczba bajtów:	7	1	2/6	2/6	2	46-1500		4

Rysunek 4-1 Struktura ramki standardu IEEE 802.3

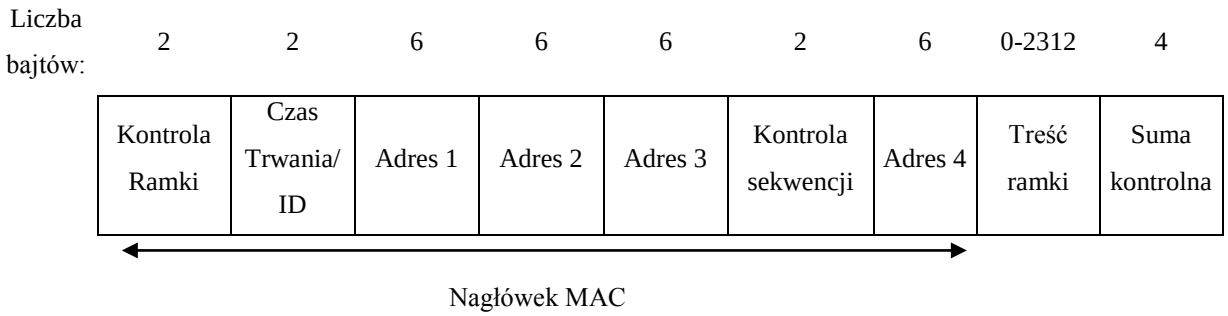
Ramka rozpoczyna się 7 bajtami preambuły (ang. preamble), która umożliwia synchronizację w warstwie fizycznej. Pole startu ramki jest ciągiem o znanej sekwencji. Następnie znajdują się pola adresowe stacji źródłowej i docelowej. Są to pola 2 lub 6 bajtowe. Kolejne pole zajmuje 2 bajty i określa długość następującego po nim pola danych. Pole danych może zgodnie ze standardem mieć długość od 46 do 1500 bajtów. Jeżeli długość jest mniejsza niż 46 bajtów wykorzystywane jest dodatkowe pole rozszerzenia (ang. pad-padding). Pole danych jest przygotowywane przez podwarstwę kanału logicznego LLC. Ostatnie czterobajtowe pole sumy kontrolnej (ang. frame check sequence, FCS) zawiera ciąg kontrolny kodu cyklicznego CRC (ang. cyclic renundancy code).

4.1.2 Ramka 802.11

Każda ramka zgodna ze standardem IEEE 802.11 składa się z następujących elementów:

a) nagłówka MAC (ang. MAC header), w skład którego wchodzą pola: Kontrola Ramki, Czas Trwania/ ID, Kontrola Sekwencji oraz pola adresowe;
b) treści ramki (ang. frame body), które zawiera informacje zależne od typu ramki;
c) sumy kontrolnej, które zawiera 32-bitowy ciąg kontrolny kodu cyklicznego CRC;

Struktura ramki została przedstawiona na Rysunku 5-2.



Rysunek 4-2 Struktura ramki standardu IEEE 802.11

Występowanie aż czterech adresów MAC, jest widocznym elementem odróżniającym ramkę 802.11 od ramki Ethernet. Nie wszystkie ramki posługują się jednak czterema polami adresowymi. Ponadto zawartość pól adresowych może być różna w zależności od typu ramki. Ramka 802.11 nie zawiera pola długości danych oraz preambuły. Preambuła jest częścią warstwy fizycznej, natomiast długość danych sygnalizowana jest w nagłówku pola danych.

4.1.3 Enkapsulacja

Enkapsulacja ma wiele znaczeń. Jednym z nich jest dopisywanie nagłówków z kolejnych warstw w czasie wędrowania danych z góry stosu protokołu na dół. Przykładowo segment TCP jest enkapsulowany w datagram IP poprzez dopisanie nagłówka IP. Przy odbiorze danych, czyli wędrowaniu ich w górę stosu protokołów następuje odwrotny proces dekapsulacji, czyli usuwanie nagłówków z kolejnych warstw w czasie wędrowania danych w górę stosu.

4.1.4 Typy ramek 802.11

Wyróżniamy trzy typy ramek 802.11:
ramki zarządzające: beacon, probe request, probe response, authentication request, authentication response, deauthentication request, association request, association response, disassociation request
ramki danych- są to właściwe ramki wewnątrz których są enkapsulowane protokoły wyższych warstw np. IP, TCP
ramki kontrolne: RTS, CTS, ACK

4.2 Funkcje warstwy MAC w 802.11

Główne funkcje warstwy MAC to skanowanie, uwierzytelnianie, przyłączanie i szyfrowanie.

1. Skanowanie- wykorzystywane jest podczas szukania punktu dostępowego przez stację kliencką. Skanowanie może być pasywne i aktywne.

Skanowanie pasywne polega na przeglądanie przez stację kliencką wszystkich kanałów w poszukiwaniu ramek typu *beacon*, rozsyłanych co jakiś czas przez punkt dostępowy. W takiej ramce znajdują się informacje między innymi o identyfikatorze SSID, kanale pracy, dostępnych szybkościach transmisji, czy sile sygnału.
Skanowanie aktywne polega na wysyłaniu przez stację kliencką ramki rozgłoszeniowej *probe request* na którą odpowiadają wszystkie punkty dostępowe będące w zasięgu ramką *probe response*. Dzięki aktywnemu skanowaniu stacja nie musi czekać na ramkę *beacon*.

2. Uwierzytelnianie- to proces ustalania tożsamości między stacjami. Wyróżniamy dwa rodzaje systemów: system otwarty i system z kluczem dzielonym, który opiera się na szyfrowaniu protokołem WEP. Ogólnie stacja wysyła ramkę *authentication request*, w odpowiedzi na którą AP odpowiada ramką *authentication reply*, zawierającą informacje o przyznaniu, bądź odmowie dostępu.

3. Przyłączanie- to proces przyłączenia się stacji klienckiej do AP, potrzebny do synchronizacji obu stron, następujący po poprawnym uwierzytelnieniu. Stacja kliencka inicjuje proces przyłączenia przez wysłanie ramki typu *association request*, w której zawiera informacje na temat obsługiwanych przepływności, czy identyfikatora SSID sieci do której chce się przyłączyć. AP rezerwuje dla danego połączenia obszar w pamięci i przydziela tzw. identyfikator przyłączenia, który jest wysyłany w ramce typu *association response*. Identyfikator przyłączenia jest używany podczas przesyłania danych.

4.3 Tryby promiscous i RF monitoring mode

Interfejs bezprzewodowy może pracować w jednym z trzech trybów:

1. tryb zwykły- w zwykłym trybie pracy interfejs odbiera ramki, których adres docelowy MAC pokrywa się z adresem MAC interfejsu. Pozostałe ramki są odrzucane, a tym samym nie są przekazywane do wyższych warstw w stosie protokołów.
Przykładowy wynik komendy *ip a* może wyglądać następująco:

```
wlan0: <BROADCAST,MULTICAST,UP> mtu 576 qdisc pfifo_fast qlen 1000
      link/ether 00:80:c8:1c:6a:51 brd ff:ff:ff:ff:ff:ff
      inet 192.168.0.10/24 brd 192.168.0.255 scope global wlan0
```

2. tryb promiscous- w trybie pracy promiscous interfejs odbiera wszystkie ramki, które do niego docierają, a więc również te, których adres docelowy MAC nie pokrywa się z adresem MAC interfejsu. Ramki te są następnie przekazywane do wyższych warstw w stosie protokołów. Najczęstszym zastosowaniem tego trybu jest sniffing, czyli podsłuchiwanie ruchu sieciowego.
Przykładowy wynik komendy *ip a* może wyglądać następująco:

```
wlan0: <BROADCAST,MULTICAST,PROMISC,UP> mtu 576 qdisc pfifo_fast qlen 1000
    link/ether 00:80:c8:1c:6a:51 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.10/24 brd 192.168.0.255 scope global wlan0
```

Wyróżnione pola PROMISC oraz ether wskazują, że karta pracuje w trybie promiscous.

3. tryb RFMON- jest to specjalny tryb „RF monitoring mode", występujący jedynie w kartach bezprzewodowych, w którym interfejs potrafi odbierać wszystkie ramki 802.11 będące w powietrzu, także ramki kontrolne i sterujące. Nie wszystkie drivery potrafią obsłużyć opisywany tryb. W czasie pracy w trybie RFMON interfejs jest odłączany od sieci.
Przykładowy wynik komendy *ip a* może wyglądać następująco:

```
wlan0: <BROADCAST,MULTICAST,PROMISC,UP> mtu 576 qdisc pfifo_fast qlen 1000
    link/[802] 00:80:c8:1c:6a:51 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.10/24 brd 192.168.0.255 scope global wlan0
```

Przykładowy wynik komendy *ifconfig* może wyglądać następująco:

```
wlan0     Link encap:UNSPEC  HWaddr 00-80-C8-1C-86-A3-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.0.18  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::280:c8ff:fe1c:86a3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10761 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:6 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4270872 (4.0 MiB)  TX bytes:574 (574.0 b)
          Interrupt:16 Base address:0xd000
```

Wytłuszczone fragmenty są charakterystyczne dla interfejsu działającego w trybie RF monitoring mode.

4.4 WEP

WEP (ang. Wired Equivalent Privacy) to protokół, którego zadaniem jest szyfrowanie w warstwie MAC danych przesyłanych drogą bezprzewodową. W założeniu miał zapewnić sieci bezprzewodowej poziom bezpieczeństwa zbliżony do sieci przewodowej, jednak szybko został złamany i obecnie jest zdecydowanie za słaby do poważnych zastosowań.

Protokół WEP opiera się na sekretnym kluczu k, który jest wspólny dla wszystkich użytkowników należących do tego samego BSS. Klucz ma długość 40, 104 lub 234 bitów, jednak z reguły posługujemy się wartościami 64, 128 i 256 bitów, które są sumą klucza i tzw. wektora IV. Szyfrowanie i deszyfrowanie wykorzystuje algorytm RC4, który jest algorytmem szyfrowania strumieniowego.

Obecnie programy takie jak Airsnort, czy WEPCrack wykorzystując odkryty błąd w algorytmie potrafią znaleźć klucz 256 bitowy po kilku godzinach. Oczywiście przy sprzyjających warunkach, tzn. przy dużej ilości przesyłanych danych.

Dużą wadą protokołu WEP, jest brak mechanizmu wymiany kluczy. Konieczność ręcznego wprowadzania klucza na każdym komputerze powoduje, że dla dużych sieci korzystanie z klucza WEP staje się bardzo uciążliwe.

Obecnie istnieje wiele mechanizmów wypierających WEP. Standard WPA gwarantuje, dynamiczną wymianę kluczy, natomiast niedawno wprowadzony standard 802.11i definiuje zupełnie nową architekturę bezpieczeństwa.

4.5 Zabezpieczenia sieci WLAN

Poniżej przedstawione zostały zabezpieczenia sieci WLAN:

- Wyłączyć w AP rozgłaszanie SSID, włączyć ukrywanie SSID o ile jest to możliwe
- Zmienić domyślne ustawienia (SSID, hasła, adres IP)
- Włączyć szyfrowanie z kluczem WEP (najlepiej przy zastosowaniu najdłuższego klucza)
- Stosować trudne do odgadnięcia klucze WEP
- Zastosować politykę częstej wymiany klucza WEP
- Stosować SSID jako hasło. Stosować trudny do odgadnięcia SSID
- Włączyć kontrolę dostępu na poziomie adresów MAC, nr IP, czy protokołów
- Wyłączyć protokół DHCP
- Stosować bezpieczne protokoły: IPSEC, SSH, 802.1X)
- Aktualizować oprogramowanie kart sieciowych i AP
- Zabezpieczyć AP przed fizycznym dostępem
- Zainstalować firewalla i system IDS

- Zastosować fałszywy punkt dostępowy w celu zmylenia przeciwnika

Należy pamiętać, że nawet najsłabsze zabezpieczenia są lepsze od braku zabezpieczeń.

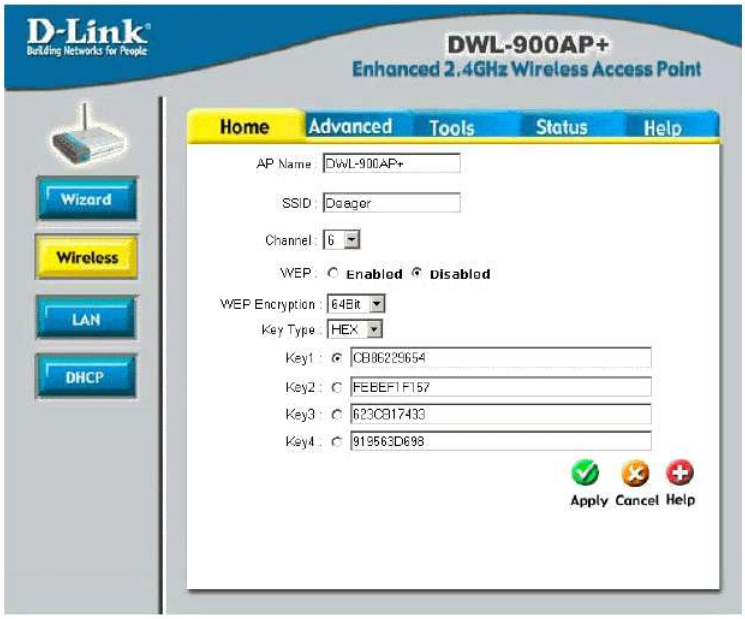
4.6 Konfiguracja punktów dostępowych

4.6.1 Konfiguracja AP firmy D-Link

Instrukcja konfigurowania punktu dostępowego firmy D-Link Dwl-900AP+ znajduje się w oficjalnym manualu do tego urządzenia. Istotny jest rozdział 5 zatytułowany „Using the Configuration Menu". Dokument zawiera zrzuty ekranu, co znacznie ułatwia zapoznanie się z możliwościami AP.

Punkt dostępowy konfiguruje się z poziomu przeglądarki internetowej (Rysunek 4-1). Poniżej podane są przykładowe opcje konfiguracyjne:

- SSID, kanał, oraz klucz WEP możemy ustawiać w zakładce Home-> Wireless
- Adres IP ustawiamy w zakładce Home-> LAN
- Rozgłaszanie SSID oraz próg RTS ustawiamy w zakładce Advanced-> Performance
- Filtrację MAC ustawiamy w zakładce Advanced-> Filters



Rysunek 4-3 Strona konfiguracyjna D-Link Dwl-900AP+