
Bezprzewodowe sieci lokalne



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI



UMCS
UNIWERSYTET MEDYCYNICZNY
W LUBLINIE

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Projekt „Programowa i strukturalna reforma systemu kształcenia na Wydziale Mat-Fiz-Inf”.
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego.

Człowiek-najlepsza inwestycja

UNIwersYTET MARIi CURIE-SKŁODOWSKIEJ
WYDZIAŁ MATEMATYKI, FIZYKI I INFORMATYKI
INSTYTUT INFORMATYKI

Bezprzewodowe sieci lokalne

Karol Kuczyński
Waldemar Suszyński



LUBLIN 2012

**Instytut Informatyki UMCS
Lublin 2012**

Karol Kuczyński
Waldemar Suszyński
BEZPRZEWODOWE SIECI LOKALNE

Recenzent: Andrzej Bobyk

Opracowanie techniczne: Marcin Denkowski
Projekt okładki: Agnieszka Kuśmierska

Praca współfinansowana ze środków Unii Europejskiej w ramach
Europejskiego Funduszu Społecznego

Publikacja bezpłatna dostępna on-line na stronach
Instytutu Informatyki UMCS: informatyka.umcs.lublin.pl.

Wydawca

Uniwersytet Marii Curie-Skłodowskiej w Lublinie
Instytut Informatyki
pl. Marii Curie-Skłodowskiej 1, 20-031 Lublin
Redaktor serii: prof. dr hab. Paweł Mikołajczak
www: informatyka.umcs.lublin.pl
email: dyrii@hektor.umcs.lublin.pl

Druk

FIGARO Group Sp. z o.o. z siedzibą w Rykach
ul. Warszawska 10
08-500 Ryki
www: www.figaro.pl

ISBN: 978-83-62773-37-4

SPIS TREŚCI

PRZEDMOWA	vii
1 PODSTAWOWE POJĘCIA	1
1.1. Wstęp	2
1.2. Architektura logiczna sieci bezprzewodowych	3
1.3. Nawiązywanie połączenia z punktem dostępowym	6
1.4. Lokalne sieci bezprzewodowe w modelu ISO/OSI	7
2 PODSTAWY FIZYCZNE	9
2.1. Fale elektromagnetyczne	10
2.2. Anteny i ich parametry	13
2.3. Pasma ISM	17
3 STANDARDY LOKALNYCH SIECI BEZPRZEWODOWYCH	21
3.1. Wstęp	22
3.2. 802.11b	22
3.3. 802.11a	23
3.4. 802.11g	23
3.5. 802.11n	24
3.6. Przyszłość standardu	24
4 MECHANIZM DOSTĘPU DO MEDIUM	27
4.1. Wstęp	28
4.2. Podstawy	28
4.3. Problem ukrytego węzła	30
4.4. RTS/CTS i fragmentacja ramek	31
4.5. Ramki 802.11	32
5 BEZPRZEWODOWE PUNKTY DOSTĘPOWE	39
5.1. Wstęp	40
5.2. Konfiguracja punktu dostępowego Cisco Aironet	41
6 BEZPIECZEŃSTWO SIECI BEZPRZEWODOWYCH	55

6.1.	Wstęp	56
6.2.	Najprostsze zabezpieczenia	57
6.3.	Zabezpieczenia kryptograficzne	58
6.4.	Monitorowanie sieci bezprzewodowej	72
6.5.	Podsumowanie	73
7	BEZPRZEWODOWE WIRTUALNE SIECI LOKALNE	75
7.1.	Wstęp	76
7.2.	Konfiguracja VLAN na punktach dostępowych Aironet	76
7.3.	Zadanie	81
7.4.	Wskazówki do zadania 7.3	82
8	PRZEKAŹNIKI I MOSTY BEZPRZEWODOWE	85
8.1.	Wstęp	86
8.2.	Mosty bezprzewodowe w otwartej przestrzeni	88
8.3.	Konfiguracja punktu dostępowego Aironet w roli przekaźnika bezprzewodowego	90
8.4.	Zadanie – przekaźnik bezprzewodowy	92
8.5.	Konfiguracja mostu bezprzewodowego z urządzeniami Aironet	92
8.6.	Zadanie – konfiguracja mostu bezprzewodowego	96
8.7.	Zadanie – konfiguracja mostu grupy roboczej	96
9	INTEGROWANIE BEZPRZEWODOWYCH ROZWIĄZAŃ W SIECIACH LOKALNYCH	99
9.1.	Wstęp	100
9.2.	Protokoły LWAPP i CAPWAP	101
9.3.	Przykładowa konfiguracja kontrolera WLAN	103
9.4.	Konfiguracja kontrolera WLAN z użyciem wiersza poleceń	107
9.5.	Konfigurowanie kontrolera WLAN przez przeglądarkę WWW	109
9.6.	Zadanie	115
10	ROZWIĄZANIA TYPU <i>open source</i> DLA SIECI BEZPRZEWODOWYCH	117
10.1.	Wstęp	118
10.2.	Możliwości alternatywnego oprogramowania	119
A	DHCP I TRANSLACJA ADRESÓW	123
A.1.	DHCP	124
A.2.	Translacja adresów	125
	BIBLIOGRAFIA	129
	SKOROWIDZ	133

PRZEDMOWA

Od wielu lat lokalne sieci komputerowe (ang. *Local Area Networks*, LAN) zdominowane są przez kolejne generacje technologii Ethernet. Niegdyś konkurencyjne rozwiązania, jak Token Ring (protokół IEEE 802.5 [1]), FDDI (ANSI X3T9.5 [2]) i ARCNET (ATA 878.1-1999 [3]) mają już jedynie znaczenie historyczne.

Od początku XXI wieku bardzo dynamicznie wzrasta popularność lokalnych sieci bezprzewodowych, działających zgodnie ze standardami IEEE 802.11, popularnie określanych mianem sieci Wi-Fi. Oczekuje się, że będą one funkcjonalnym odpowiednikiem tradycyjnych sieci lokalnych, przy czym okablowanie łączące poszczególne urządzenia (a przynajmniej znaczna jego część) jest wyeliminowane dzięki transmisji bezprzewodowej, za pośrednictwem fal radiowych.

Dostępne obecnie technologie lokalnych sieci bezprzewodowych pod wieloma względami ustępują sieciom przewodowym. Są znacznie wolniejsze, mniej stabilne i niezawodne. Ciągłe aktualną kwestią jest zapewnienie odpowiedniego poziomu bezpieczeństwa. Problemy te zostaną dokładniej przedstawione w kolejnych rozdziałach tego podręcznika. Jednak nawet bardzo pobieżna analiza rynku urządzeń sieciowych dowodzi, że już na obecnym etapie rozwoju sieci bezprzewodowych, ich niezaprzeczalne zalety są w stanie zrekomensować z nawiązką pewne niedogodności. Odnosi się to do niewielkich sieci domowych, małych biur, jak również największych sieci korporacyjnych.

Początkowe rozdziały podręcznika zawierają teoretyczne wprowadzenie do technologii lokalnych sieci bezprzewodowych. Przedstawione są fizyczne podstawy transmisji radiowej, standardy, mechanizmy dostępu do medium, problemy bezpieczeństwa w kolejnych generacjach protokołów rodziny 802.11. Omówiony jest sposób konfigurowania bezprzewodowych punktów dostępowych, w podstawowym i nieco bardziej zaawansowanym zakresie. Kolejne zagadnienia to repeatery i mosty bezprzewodowe oraz bezprzewodowe wirtualne sieci LAN (VLAN). Zaproponowano szereg ćwiczeń praktycznych, możliwych do wykonania w laboratorium sieciowym, wyposażonym w urządzenia jednego z wiodących producentów (bezprzewodowe punk-

ty dostępne Aironet oraz przełączniki Catalyst, produkowane przez Cisco Systems). Nieco uwagi poświęcono także alternatywnym rozwiązaniom typu *open source*.

Zakładamy, że czytelnikowi znane są już podstawowe zagadnienia związane z routowaniem [4, 5] i przełączaniem w sieciach lokalnych, wirtualnymi sieciami LAN (VLAN) [6, 7], jak również sposób konfiguracji urządzeń Cisco z systemem IOS.

Z oczywistych względów, wiele zagadnień musiało zostać pominiętych lub przedstawionych pobieżnie. Jednak zawarty tu zasób wiedzy powinien wystarczyć do samodzielnej budowy prostych sieci bezprzewodowych, jak również stanowić podstawę do studiowania bardziej zaawansowanych aspektów technologii. Więcej informacji można znaleźć w cytowanej dokumentacji technicznej i opisach standardów, jak również w literaturze uzupełniającej [8, 9, 10, 11, 12, 13, 14, 15].

ROZDZIAŁ 1

PODSTAWOWE POJĘCIA

1.1.	Wstęp	2
1.2.	Architektura logiczna sieci bezprzewodowych	3
1.2.1.	IBSS	3
1.2.2.	BSS	3
1.2.3.	ESS	4
1.3.	Nawiązywanie połączenia z punktem dostępowym	6
1.4.	Lokalne sieci bezprzewodowe w modelu ISO/OSI	7

1.1. Wstęp

Bezprzewodowe sieci lokalne są alternatywą dla konwencjonalnych rozwiązań sieci LAN (czyli obecnie przede wszystkim dla technologii Ethernet), pozbawioną ograniczeń wynikających z konieczności prowadzenia okablowania. Istnieją również rozwiązania bezprzewodowe dla innych rodzajów sieci, np.:

- Bluetooth i IrDA są przykładami sieci osobistych (ang. *Personal Area Network*, PAN), o zasięgu do kilku metrów.
- Bezprzewodową technologią dla sieci metropolitalnych (MAN) jest WiMAX (standard IEEE 802.16 [17]). Zapewnia on szybki dostęp do sieci i zasięg rzędu kilkudziesięciu kilometrów. Może być również alternatywą dla sieci komórkowych. Wiele wskazywało, że WiMAX stanie się powszechnym sposobem dostępu do Internetu dla użytkowników indywidualnych. Obecnie jednak wzrasta tu zainteresowanie technologią LTE (*Long Term Evolution*), wywodzącą się wprost z GSM/GPRS/UMTS, oferującą lepsze parametry.
- Do bezprzewodowych technologii sieci rozległych (WAN) można zaliczyć telefonię komórkową GSM, GPRS, UMTS, różnego rodzaju łącza satelitarne.



Rysunek 1.1. Logo Wi-Fi CERTIFIED™ – zastrzeżony znak towarowy Wi-Fi Alliance®

Przedmiotem tego podręcznika są tylko bezprzewodowe sieci lokalne. Powszechnie są one określane mianem Wi-Fi (*Wireless Fidelity*). W rzeczywistości, dobrze znane logo Wi-Fi (rys. 1.1) jest znakiem towarowym

Wi-Fi Alliance¹ (dawniej WECA, *Wireless Ethernet Compatibility Alliance*) – stowarzyszenia zrzeszającego firmy produkujące urządzenia sieciowe. Jego celem jest promowanie standardu IEEE 802.11 [16], dbanie o zgodność urządzeń ze standardem oraz ich certyfikacja. Zatem obecność logo Wi-Fi na obudowie urządzenia świadczy o tym, że zostało ono przetestowane pod kątem zgodności z 802.11. Oczywiście brak takiego symbolu nie musi oznaczać braku zgodności ze standardem.

1.2. Architektura logiczna sieci bezprzewodowych

1.2.1. IBSS



Rysunek 1.2. Bezprzewodowa sieć *ad-hoc* (IBSS)

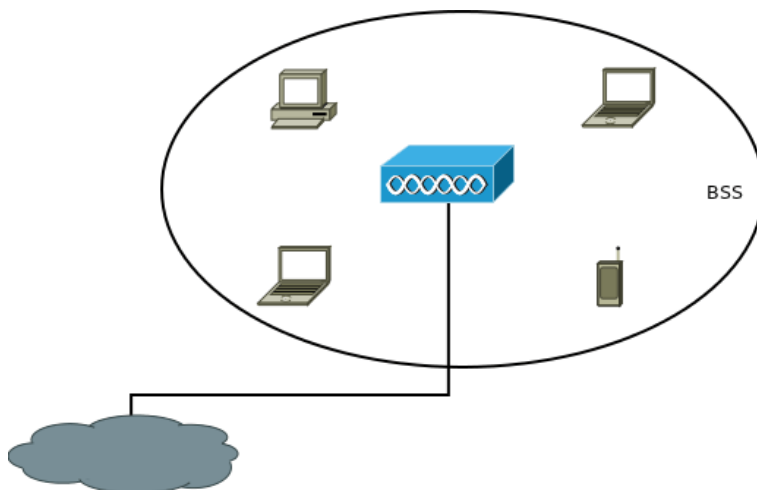
Najprostsza sieć bezprzewodowa może być zbudowana z kilku równorzędnych hostów, wyposażonych w bezprzewodowe karty sieciowe (rys. 1.2), bez żadnych dodatkowych urządzeń kierujących ruchem (tzw. sieć *ad-hoc*). Poszczególne hosty komunikują się ze sobą bezpośrednio. To rozwiązanie jest określane mianem sieci niezależnej (ang. *Independent Basic Service Set*, IBSS). Miewa zastosowanie w przypadku potrzeby wymiany danych między nie więcej niż kilkoma urządzeniami. Poszczególne urządzenia muszą mieć skonfigurowany ten sam identyfikator sieci – SSID (ang. *Service Set Identifier*), złożony maksymalnie z 32 znaków. Jest on przesyłany w postaci jawnego tekstu.

1.2.2. BSS

Podstawowym typem sieci bezprzewodowej jest BSS (ang. *Basic Service Set*, podstawowy zestaw usług), określane też mianem trybu infrastrukturalnego (ang. *infrastructure mode*). Poszczególne urządzenia w sieci nie komunikują się ze sobą bezpośrednio (jak w przypadku IBSS), lecz poprzez specjalne urządzenie – punkt dostępowy (ang. *access point*) – rys. 1.3. Może on zapewniać również połączenie z siecią przewodową.

Wszystkie urządzenia w sieci BSS (hosty i punkt dostępowy) muszą mieć skonfigurowany ten sam SSID. Ponadto, sieć posiada również unikalny identyfikator BSSID (ang. *Basic Service Set Identifier*). Najczęściej jest on

¹ <http://www.wi-fi.org/>



Rysunek 1.3. Sieć typu BSS

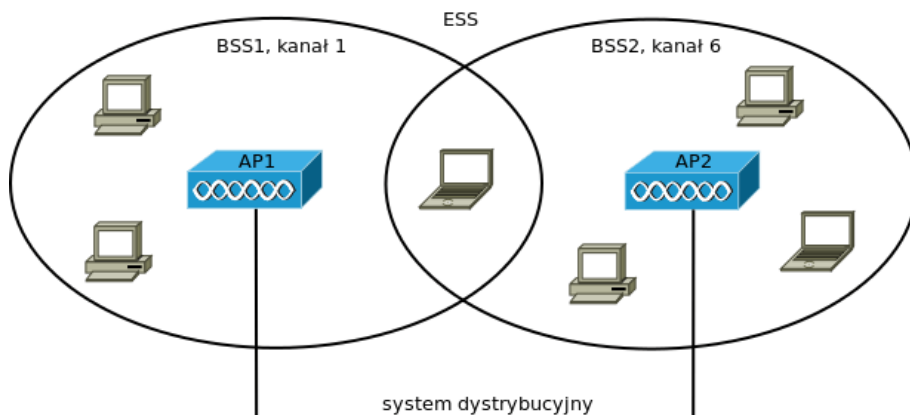
identyczny z 48-bitowym adresem MAC interfejsu radiowego punktu dostępowego (w przypadku IBSS jest losowy).

1.2.3. ESS

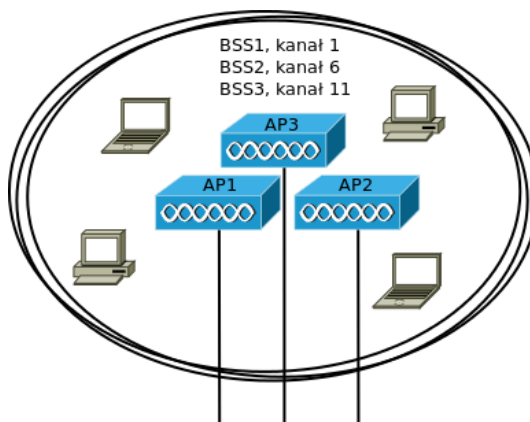
Przy rozbudowie sieci bezprzewodowej może okazać się, że jeden punkt dostępowy nie jest w stanie zapewnić dostępu do sieci w całym obszarze, w którym jest to wymagane, lub z powodu dużej liczby hostów przepustowość sieci jest niewystarczająca. Instaluje się wówczas kolejne punkty dostępowe – rys. 1.4. Są one połączone ze sobą oraz z pozostałą częścią sieci poprzez tzw. system dystrybucyjny, najczęściej przewodowy, w technologii Ethernet. Jeżeli problemem nie jest zasięg sieci, lecz przepustowość, kilka punktów dostępowych może zostać zainstalowanych w tym samym miejscu – rys. 1.5. W ten sposób uzyskuje się skalowalność sieci bezprzewodowej.

Wszystkie punkty dostępowe mają ten sam SSID (który bywa określanym mianem ESSID), natomiast różne BSSID. Jeżeli sieć ma być dostępna w całym obszarze, zasięgi poszczególnych punktów dostępowych muszą częściowo pokrywać się. Aby nie zakłócały się wzajemnie, trzeba użyć różnych (odpowiednio odległych) kanałów radiowych. Host znajdujący się w zasięgu więcej niż jednego punktu dostępowego, zwykle łączy się wtedy z tym, którego sygnał jest najsilniejszy (mechanizm wyboru punktu dostępowego nie jest sprecyzowany w standardzie i zależy od producenta sprzętu).

Komputer użytkownika, który przemieszcza się z obszaru BSS1 do BSS2, w pewnym momencie straci połączenie z AP1 i nawiąże z AP2. Pod pojęciem roamingu rozumiemy tu takie przeprowadzenie tej operacji, by było to



Rysunek 1.4. Sieć typu ESS



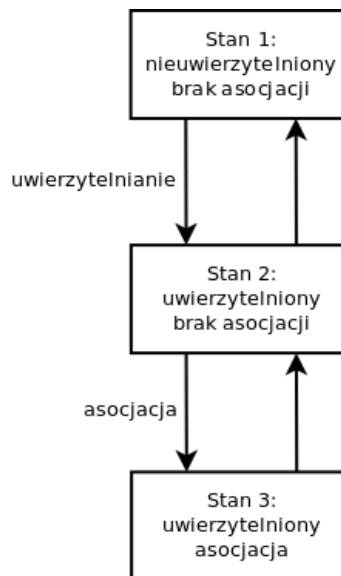
Rysunek 1.5. Kilka BSS w tym samym obszarze

niezauważalne dla użytkownika (ang. *seamless roaming*). Nie powinna więc trwać dłużej niż kilka dziesiątych sekundy, a komputer powinien zachować ustawienia IP. Dzięki temu, nie zostaną przerwane nawiązane połączenia sieciowe i zachowana będzie np. ciągłość rozmowy prowadzonej przy użyciu VoIP. Implementacja roamingu wymaga odpowiedniego mechanizmu do komunikacji między punktami dostępowymi. Można wykorzystać protokół IAPP (ang. *Inter Acces Point Protocol*). W 2003 roku IEEE przedstawiło propozycję opisującego go standardu – 802.11f [18], jednak w 2006 roku została ona odrzucona. W związku z tym, nadal poszczególni producenci mogą stosować własne rozwiązania.

1.3. Nawiązywanie połączenia z punktem dostępowym

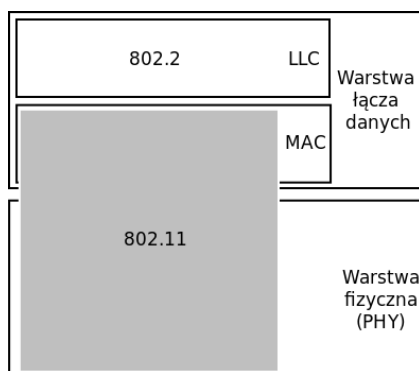
Połączenie z siecią Ethernet dokonuje się poprzez elektryczne połączenie karty sieciowej z portem przełącznika. Analogiczna operacja w sieci bezprzewodowej, czyli połączenie hosta z punktem dostępowym, jest znacznie bardziej skomplikowana. Musi zostać przeprowadzona zdalnie, przy pomocy odpowiednich ramek zarządzających. Można tu wyróżnić 3 stany – rys. 1.6.

1. Początkowo (stan 1) host nie jest uwierzytelniony ani w jakikolwiek sposób powiązany z punktem dostępowym (lub innym hostem w przypadku IBSS). Następuje proces uwierzytelniania, przy czym standard 802.11 dopuszcza dwa warianty. System otwarty zezwala na dostęp każdemu urządzeniu, które zgłosi takie żądanie, bez żadnej weryfikacji. Drugim wariantem jest uwierzytelnianie ze współdzielonym kluczem – następuje sprawdzenie, czy oba urządzenia dysponują identycznym kluczem.
2. W razie pomyślnego uwierzytelnienia, host będąc w stanie 2., może wysłać prośbę o dokonanie asocjacji. W odpowiedzi otrzymuje między innymi swój logiczny numer portu (ang. *Association ID*)), który możemy potraktować jako odpowiednik numeru portu przełącznika Ethernet.
3. W trzecim stanie host może już wysyłać i odbierać dane. Host może być jednocześnie uwierzytelniony na kilku punktach dostępowych, natomiast asocjacja może nastąpić tylko z jednym.



Rysunek 1.6. Nawiązywanie połączenia z siecią bezprzewodową

1.4. Lokalne sieci bezprzewodowe w modelu ISO/OSI



Rysunek 1.7. Protokoły lokalnych sieci bezprzewodowych w modelu ISO/OSI

Zagadnienia lokalnych sieci bezprzewodowych, tak samo jak w przypadku jakichkolwiek sieci lokalnych, dotyczą dwóch najniższych warstw modelu ISO/OSI (rys. 1.7). Obecnie powszechnie przyjęte są tu standardy IEEE (*Institute of Electrical and Electronics Engineers*)². W przypadku wszystkich tych technologii (w tym między innymi bezprzewodowych sieci lokalnych i tzw. Ethernetu), działanie podwarstwy LLC określa standard 802.2 [19]. Standard sieci bezprzewodowych 802.11 odnosi się do podwarstwy MAC oraz warstwy fizycznej (PHY). Poszczególne, współcześnie wykorzystywane warianty lokalnych sieci bezprzewodowych 802.11 wykorzystują identyczną implementację podwarstwy MAC, natomiast różnią się warstwą fizyczną.

² <http://www.ieee.org/>

ROZDZIAŁ 2

PODSTAWY FIZYCZNE

2.1. Fale elektromagnetyczne	10
2.2. Anteny i ich parametry	13
2.3. Pasma ISM	17

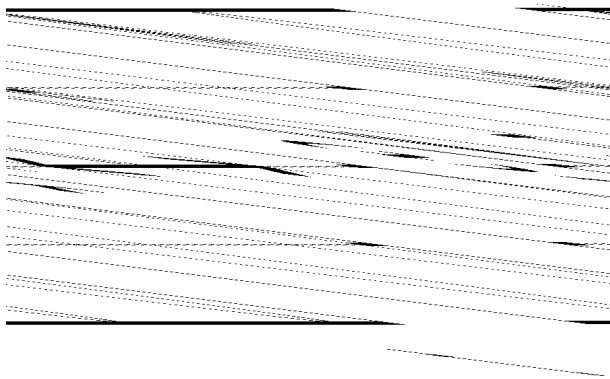
2.1. Fale elektromagnetyczne

W bezprzewodowych sieciach lokalnych transmisja odbywa się za pośrednictwem fal elektromagnetycznych. Bieżący rozdział zawiera informacje o podstawach fizycznych transmisji radiowej. Przedstawione są jedynie te zagadnienia, które są najistotniejsze z praktycznego punktu widzenia, przy projektowaniu, budowie i zarządzaniu sieciami bezprzewodowymi. W związku z tym, wiele problemów zostało pominiętych, przedstawionych skrótowo lub w uproszczeniu.

Rys. 2.1 przedstawia wykres fali sinusoidalnej, opisanej wzorem:

$$y(t) = A \sin(\omega t + \phi) \quad (2.1)$$

A oznacza amplitudę fali, T – okres, ω – częstość kołową (zdefiniowaną dalej), t – czas, a ϕ – przesunięcie fazowe.



Rysunek 2.1. Wykres fali sinusoidalnej

Częstotliwość fali określa liczbę cykli w jednostce czasu:

$$f = 1/T \quad (2.2)$$

Jednostką częstości jest 1 herc (Hz). W zakresie częstości wykorzystywanych w przypadku sieci bezprzewodowych, zwykle stosuje się jednostki pochodne: megaherc

$$1MHz = 10^6 Hz \quad (2.3)$$

i gigaherc:

$$1GHz = 10^9 Hz \quad (2.4)$$

Bywa wykorzystywana także częstość kołowa:

$$\omega = 2\pi/T \quad (2.5)$$

W przypadku fali elektromagnetycznej, mamy do czynienia z rozchodzącymi się oscylacjami pola elektrycznego i magnetycznego, które są do siebie prostopadłe. Jeżeli drgania wektora pola elektrycznego odbywają się w jednej płaszczyźnie, w kierunku prostopadłym do kierunku rozchodzenia się fali, mówimy o polaryzacji liniowej. W lokalnych sieciach bezprzewodowych zwykle stosuje się polaryzację liniową w kierunku pionowym (V), znacznie rzadziej poziomym (H).

Fala elektromagnetyczna w próżni rozchodzi się z tzw. prędkością światła:

$$c = 299792458 \text{ m/s} \approx 3 \cdot 10^8 \text{ m/s} \quad (2.6)$$

natomiast w powietrzu nieco wolniej (co akurat w przypadku transmisji w lokalnych sieciach bezprzewodowych jest pomijalne).

Długość fali jest to najmniejsza odległość między dwoma punktami o tej samej fazie drgań (tzn. identycznej wartości i kierunku wychylenia). Długość fali λ , prędkość i częstotliwość są związane zależnością:

$$c = \lambda f \quad (2.7)$$

Aby falę elektromagnetyczną wykorzystać do transmisji informacji, należy dokonać jej modulacji. W radiofonii stosuje się najczęściej modulację amplitudy (np. fale długie, krótkie i średnie) lub częstotliwości (UKF). Można też dokonywać zmiany fazy sygnału (modulacja fazy).

Techniki modulacji stosowane we współczesnej komunikacji cyfrowej są natomiast znacznie bardziej skomplikowane. Do transmisji nie jest wykorzystywana jedna fala nośna o określonej częstotliwości, lecz cały zakres częstotliwości. Im większa szerokość dostępnego pasma analogowego (tzn. zakres dostępnych częstotliwości, wyrażony w hercach), tym większa szerokość pasma cyfrowego, tzn. ilość danych, które można przesłać w jednostce czasu (wyrażona w bitach na sekundę).

Jednym z podstawowych parametrów emitowanego sygnału jest moc, zdefiniowana jako pochodna energii po czasie:

$$P = dE/dt \quad (2.8)$$

wyrażona w watach (W). W przypadku prądu elektrycznego, moc wyraża się wzorem:

$$P = UI \quad (2.9)$$

gdzie U jest napięciem a I natężeniem. Moc sygnału emitowanego przez urządzenia w lokalnych sieciach bezprzewodowych zwykle nie przekracza 100 miliwatów ($1 \text{ mW} = 10^{-3} \text{ W}$).

Wraz z oddalaniem się od źródła sygnału, maleje odbierana moc. Z kolei w przypadku zastosowania wzmacniacza lub anteny, może nastąpić wzmocnienie sygnału. Ze względu na szeroki zakres zmian, który nas interesuje,

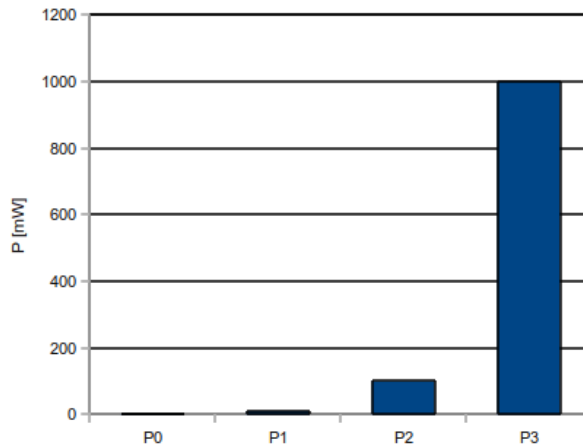
wygodnie jest użyć skali logarytmicznej. Stosunek dwóch mocy (lub innych wartości) wyraża się w decybelach ($1dB = 0,1B$):

$$P_{dB} = 10 \log_{10} \frac{P}{P_0}, \quad (2.10)$$

gdzie P jest wartością mierzoną, natomiast P_0 – poziomem odniesienia.

Załóżmy, że zostały zmierzone następujące moce sygnału:

$$P_0 = 1mW, P_1 = 10mW, P_2 = 100mW, P_3 = 1000mW \quad (2.11)$$



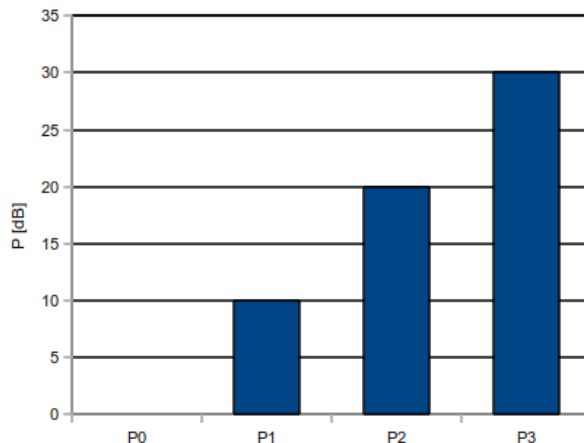
Rysunek 2.2. Przykładowe wartości mocy wyrażone w skali liniowej (w miliwatach)

Jeżeli te wartości przedstawimy na wykresie, to różnica między $1mW$ a $10mW$ będzie prawie niewidoczna (rys. 2.2). Po przeliczeniu na dB , względem P_0 , otrzymamy:

$$P_{db0} = 0dB, P_{db1} = 10dB, P_{db2} = 20dB, P_{db3} = 30dB \quad (2.12)$$

co można już w sposób czytelny przedstawić na wykresie (rys. 2.3). Wzrost lub spadek o $3dB$ odpowiada dwukrotnemu wzrostowi lub spadkowi mocy, odpowiednio, natomiast o $10dB$ – dziesięciokrotnemu.

Bywa stosowana także jednostka miary mocy względem $1mW$, czyli dBm . We wzorze 2.10 $P_0 = 0,001W$. Wówczas, przykładowo $0,001mW$ to $-30dBm$.



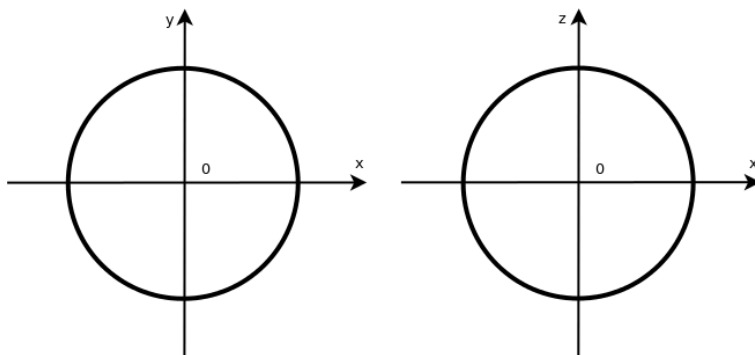
Rysunek 2.3. Przykładowe wartości mocy wyrażone w skali logarytmicznej (w decybelach)

2.2. Anteny i ich parametry

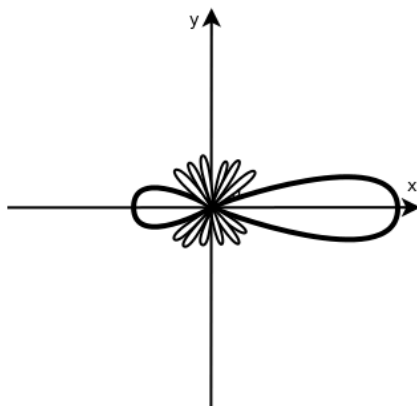
Niezbędnym elementem każdego systemu komunikacji radiowej jest antena, zamieniająca sygnał elektryczny na falę elektromagnetyczną (podczas nadawania) i odwrotnie (podczas odbioru). Antenę charakteryzuje wiele parametrów. Z punktu widzenia projektanta sieci bezprzewodowych, najważniejsza jest charakterystyka kierunkowa anteny, zysk energetyczny, polaryzacja oraz zakres przenoszonych częstotliwości (w przypadku sieci 802.11 – pasmo 2,4GHz lub 5GHz). Parametry te odnoszą się w takim samym stopniu do emisji, jak też odbierania sygnału. Powinny znaleźć się w dokumentacji technicznej udostępnionej przez producenta.

Pod względem charakterystyki promieniowania, można anteny podzielić na dookólne, emitujące promieniowanie we wszystkich kierunkach, i kierunkowe, które większość promieniowania emitują w niewielki kąt bryłowy. Są też anteny o charakterystyce pośredniej, które trudno jednoznacznie zakwalifikować jednej z tych dwóch grup. Anten dookólnych używa się w celu zapewnienia dostępu do sieci bezprzewodowej w niewielkim obszarze wokół anteny. Anteny emitujące bardzo wąską wiązkę promieniowania znajdują zastosowanie przy budowie tzw. połączeń mostowych (ang. *wireless bridge*), między miejscami oddalonymi o siebie o kilka lub więcej kilometrów.

Antena emituje energię, która jest do niej dostarczana. Zatem zysk energetyczny należy rozumieć inaczej niż dla wzmacniacza. Przy danej mocy sygnału dostarczanego do anteny, najniższym zyskiem charakteryzowałaby się antena izotropowa, emitująca promieniowanie z takim samym natężeniem



Rysunek 2.4. Charakterystyka kierunkowa anteny izotropowej



Rysunek 2.5. Przykładowa charakterystyka anteny kierunkowej

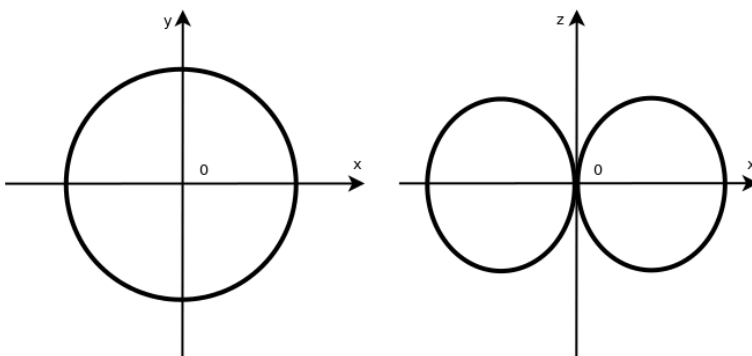
w każdym kierunku (w rzeczywistości taka antena nie istnieje) – rys. 2.4. Wzmocnienie uzyskuje się poprzez większą emisję promieniowania w określonym kierunku, kosztem mniejszej emisji w pozostałych kierunkach. Największym zyskiem energetycznym charakteryzują się zatem anteny o silnie kierunkowej charakterystyce (rys. 2.5). Uzyskuje się przy ich pomocy duży zasięg, jednak tylko w jednym kierunku. Nie nadają się więc, w przeciwieństwie do anten dookólnych, do zapewnienia dostępu do sieci bezprzewodowej grupie użytkowników w typowych warunkach biurowych lub domowych.

Zysk energetyczny anteny (ang. *gain*, G) można wyrazić w decybelach, w porównaniu z teoretyczną anteną izotropową, dla kierunku w którym antena emituje promieniowanie o największym natężeniu (lub, co jest równoważne, wykazuje najwyższą czułość przy odbieraniu) – oznaczenie dB_i . Antena izotropowa charakteryzuje się zatem zyskiem energetycznym $0dB_i$.

Najprostszą do zbudowania, najtańszą i jednocześnie najczęściej wyko-



Rysunek 2.6. Standardowa antena dipolowa



Rysunek 2.7. Charakterystyka kierunkowa anteny dipolowej

rzystywaną jest antena dipolowa. Jest to antena dookólna, charakteryzująca się najniższym spośród istniejących anten zyskiem energetycznym, wynoszącym $2,15\text{dBi}$. Charakterystykę kierunkową anteny dipolowej przedstawia rys. 2.7. W przypadku idealnego dipola, promieniowanie nie jest w ogóle emitowane w kierunku pionowym, dzięki czemu, w porównaniu z anteną izotropową, uzyskuje się większy zysk energetyczny w płaszczyźnie poziomej.

Zysk energetyczny można również podawać względem anteny dipolowej – w jednostkach dBd . Możemy zapisać, że zysk energetyczny anteny dipolowej wynosi:

$$0\text{dBd} = 2,15\text{dBi} \quad (2.13)$$

Zatem do przeliczania między dBi i dBd możemy użyć formuły:

$$G[\text{dBi}] = G[\text{dBd}] + 2,15 \quad (2.14)$$

Komunikujące się ze sobą urządzenia mogą wykorzystywać anteny o różnych charakterystykach kątowych i wzmocnieniu. Istotne jest natomiast za-

chowanie tej samej polaryzacji. W przypadku wielu typów anten możliwe są różne sposoby montażu, skutkujące różną polaryzacją, na co należy zwrócić uwagę przy pracach instalacyjnych.

Ważnym parametrem charakteryzującym transmisję radiową jest równoważna (lub według niektórych źródeł efektywna lub ekwiwalentna) moc promieniowana izotropowa (ang. *Effective Isotropic Radiated Power*, EIRP). Interpretujemy ją jako moc, którą musiałaby wypromieniować antena izotropowa, by w odbiorniku uzyskać taki sygnał, jaki generuje badana antena, w kierunku jej maksymalnego promieniowania.

Dopuszczalna prawnie w większości krajów europejskich (zgodnie ze standardem ETSI) maksymalna wartość EIRP w paśmie 2,4GHz wynosi $20dBm$, natomiast w Stanach Zjednoczonych (standard FCC) $36dBm$, a w Chinach $10dBm$. EIRP dla danego nadajnika i anteny można wyznaczyć korzystając z formuły:

$$EIRP[dBm] = P[dBm] - T_k[dB] + G_i[dBi], \quad (2.15)$$

gdzie P oznacza moc nadajnika, T_k – tłumienie kabla, natomiast G_i – zysk anteny w stosunku do izotropowej. Zakładając więc, że dysponowalibyśmy (nieistniejącą w rzeczywistości) anteną izotropową i bezstratnym połączeniem anteny z nadajnikiem, z powyższego wzoru wynika, że moglibyśmy w Europie użyć maksymalnej mocy $100mW$, natomiast w Stanach Zjednoczonych aż $4W$. O ile w warunkach domowych lub biurowych moc tego rzędu jest w zupełności wystarczająca, możliwość użycia większych mocy ułatwia budowanie mostów bezprzewodowych, jednocześnie utrudniając znalezienie niezakłócanego kanału w większych aglomeracjach.

Załóżmy teraz, że dysponujemy anteną o dość silnie kierunkowej charakterystyce, np. anteną Yagi, o zysku $13,5dBi$, dołączoną do nadajnika o mocy $15mW$, przy użyciu 10 metrów kabla o tłumienności $5,5dB/m$. W związku z tym,

$$P[dBm] = 10 \log_{10} \frac{15mW}{1mW} = 11,76dBm \quad (2.16)$$

$$T_k = 5,5dB \quad (2.17)$$

$$G_i = 13,5dBi \quad (2.18)$$

Podstawiając do wzoru 2.15 otrzymamy $EIRP = 19,76dBm$. Pomimo bardzo małej mocy nadajnika (mniejszej od mocy małej, typowej diody świecącej (LED)), wynik jest tylko nieco niższy od dopuszczalnego w Europie maksimum.

Anteny są bardzo zróżnicowane pod względem budowy. Najpopularniejsze w sieciach bezprzewodowych typy anten to:

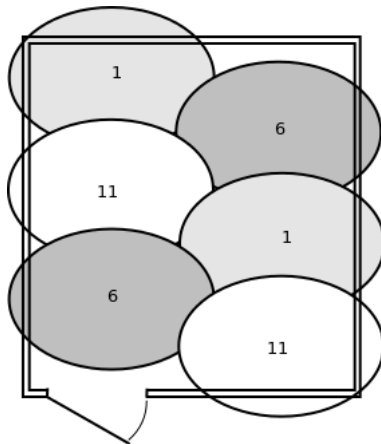
- wspomniana powyżej antena dipolowa (rys. 2.6) i różne jej modyfikacje,
- antena panelowa – płaska antena o zysku energetycznym od kilku do kilkunastu dBi, często hermetycznie zamknięta, zbudowana z dipola lub kilku połączonych dipoli oraz ekranu skupiającego promieniowanie; może być montowana do płaskich powierzchni, np. do ściany,
- antena Yagi – powszechnie stosowana do odbioru analogowej telewizji naziemnej; anteny przeznaczone dla sieci bezprzewodowych są znacznie mniejsze (ze względu na mniejszą długość fali) i często obudowane; antena charakteryzuje się zyskiem około 10-14dBi,
- antena reflektorowa, wyposażona w reflektor, najczęściej o kształcie parabolicznym; charakteryzuje się dużym zyskiem energetycznym (nawet powyżej 20dBi); tego typu anteny są powszechnie stosowane do odbioru telewizji satelitarnej,
- różnego rodzaju amatorskie konstrukcje, których opisy można łatwo znaleźć w Internecie.

Urządzenia bezprzewodowe (w szczególności punkty dostępowe i hosty) mogą posiadać anteny wbudowane (co jest powszechne w przypadku laptopów, tabletów, smartfonów, a coraz częściej także punktów dostępowych przeznaczonych do użytku wewnątrz pomieszczeń) lub możliwość dołączenia anten zewnętrznych. Standard 802.11n (przedstawiony w kolejnym rozdziale) przewiduje możliwość jednoczesnego wykorzystywania wielu anten. W przypadku starszych urządzeń (802.11a, b, g), jeżeli występuje więcej niż jedna antena, o wyborze jednej z nich decyduje administrator, lub automatycznie wybierana jest antena zapewniająca najlepszą transmisję. Należy też unikać uruchamiania interfejsu radiowego bez dołączonej anteny.

2.3. Pasma ISM

W większości przypadków emisja sygnału na falach radiowych wymaga posiadania odpowiednich licencji i pozwoleń. Jednak kilka zakresów częstotliwości pozostawiono do swobodnego wykorzystywania, pod warunkiem nieprzekraczania określonej mocy. Dostępność poszczególnych częstotliwości i szczegółowe warunki ich wykorzystywania zależą od przepisów w poszczególnych krajach.

Lokalne sieci bezprzewodowe wykorzystują część pasma ISM (ang. *industrial, scientific and medical*, pasmo przemysłowe, naukowe i medyczne), w zakresie 2,4GHz oraz 5GHz. W większości krajów świata dostępna jest przynajmniej część tego pasma. Ze względu na swobodę korzystania z niego, urządzenia powinny być możliwie odporne na zakłócenia pochodzące od innych urządzeń pracujących w tym samym paśmie. Oprócz lokalnych sieci bezprzewodowych, pasmo 2,4GHz jest wykorzystywane przez technologie



Rysunek 2.8. Przykładowy sposób użycia niezakłócających się kanałów w paśmie 2,4GHz, w sytuacji gdy do zapewnienia dostępu do sieci konieczne jest użycie wielu punktów dostępowych (ESS)

Tabela 2.1. Kanały w paśmie 2,4GHz [16]

Numer kanału	Centralna częstotliwość [MHz]
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

Bluetooth, telefony bezprzewodowe, myszy i klawiatury bezprzewodowe, piloty zdalnego sterowania, zabawki. Silne zakłócenia generują także kuchenki mikrofalowe.

Pasmo 2,4GHz zostało podzielone na 14 kanałów, co 5MHz (oprócz ostatniego). Są one przedstawione w tabeli 2.1. W większości krajów (w tym w Polsce) dostępne są kanały 1-13, w Stanach Zjednoczonych 1-11, a w Japo-

nii 1-14, przy czym w przypadku 14. kanału narzucone są pewne dodatkowe warunki.

Podczas transmisji zgodnej z 802.11, wykorzystywane są kanały o szerokości około 20MHz . Aby uniknąć wzajemnego zakłócania się przez sąsiednie sieci, należy korzystać z kanałów odpowiednio oddalonych od siebie. Całkowita separacja transmisji możliwa jest w przypadku kanałów nr 1, 6 i 11 (rys. 2.8). Nieco gorszym, ale również dopuszczalnym rozwiązaniem jest skorzystanie z kanałów nr 1, 5, 9, 13.

W paśmie 5GHz występuje znacznie większa liczba kanałów, przy czym dostępność i zasady korzystania z nich są bardziej zróżnicowane w poszczególnych krajach, niż w paśmie $2,4\text{GHz}$. W przypadku niektórych kanałów, może być obowiązkowa implementacja dodatkowych mechanizmów dynamicznego wyboru częstotliwości (ang. *dynamic frequency selection*, DFS) i sterowania mocą sygnału (ang. *transmit power control*, TPC), by uniknąć zakłócania systemów wojskowych i meteorologicznych.

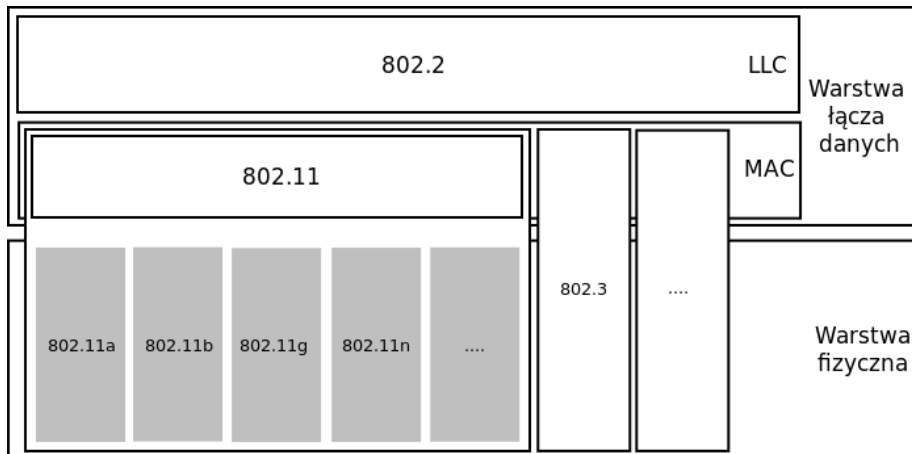
ROZDZIAŁ 3

STANDARDY LOKALNYCH SIECI BEZPRZEWODOWYCH

3.1. Wstęp	22
3.2. 802.11b	22
3.3. 802.11a	23
3.4. 802.11g	23
3.5. 802.11n	24
3.6. Przyszłość standardu	24

3.1. Wstęp

Pierwszym standardem lokalnych sieci bezprzewodowych był 802.11-1997. Wcześniej funkcjonowały własne rozwiązania poszczególnych producentów. Standard określił transmisję z szybkością 1-2 Mbit/s, przy wykorzystaniu fal radiowych z zakresu 2,4GHz lub podczerwieni. Transmisja w podczerwieni szybko okazała się niepraktyczna, chociaż wprowadzenie pokrewnej technologii IrDA¹ można uznać za sukces.



Rysunek 3.1. 802.11 w modelu ISO/OSI

Pierwsza wersja standardu 802.11 nie rozpowszechniła się, między innymi ze względu na szybkie opracowanie kolejnych: 802.11*a*, *b*, *g*, *n*. Wprowadzane zmiany dotyczyły implementacji warstwy fizycznej (PHY), podczas gdy format ramki i podstawy mechanizmu dostępu do medium (CSMA/CA) pozostały niezmienione (rys. 3.1).

3.2. 802.11b

802.11b [20] powstał jako bezpośrednie rozwinięcie początkowej wersji standardu 802.11. W warstwie fizycznej wykorzystuje się tu modulację CCK (ang. *Complementary Code Keying*), która z kolei jest rozszerzeniem stosowanej początkowo techniki DSSS (ang. *Direct-Sequence Spread Spectrum*, bezpośrednie modulowanie nośnej sekwencją kodową)

Jest to pierwszy wariant standardu, który ze względu na zadowalającą szybkość transmisji i coraz niższe ceny urządzeń uzyskał powszechną akcep-

¹ <http://www.irda.org/>

tację na całym świecie. Pierwsze urządzenia pojawiły się na rynku w 1999 roku, a wiele sieci w standardzie 802.11b funkcjonuje nadal.

Wykorzystywane jest pasmo 2,4GHz. Dzięki większej długości fali niż w 802.11a (5GHz), uzyskuje się nieco większy zasięg transmisji. Jednocześnie jednak w paśmie 2,4GHz działa wiele popularnych urządzeń, które mogą zakłócać transmisję (co zostało już omówione w Rozdziale 2). Pasma 5GHz jest obecnie wykorzystywane w mniejszym stopniu.

Maksymalna szybkość transmisji to 11 Mbit/s, chociaż ze względu na narzut związany z działaniem protokołu osiąga się przepustowości rzędu 50% teoretycznej wartości. Problem ten dotyczy także pozostałych standardów. Gdy wraz ze wzrostem odległości między komunikującymi się urządzeniami maleje moc odbieranego sygnału, automatycznie zmniejszana jest także szybkość transmisji, w celu zapewnienia odpowiedniej niezawodności.

3.3. 802.11a

Standard 802.11a [21] został ratyfikowany w 1999 roku, podobnie jak 802.11b. Ze względu na początkowe problemy z produkcją urządzeń działających w paśmie 5GHz, które jest tu wykorzystywane, pierwsze produkty pojawiły się na rynku w momencie gdy standard 802.11b miał już ugruntowaną pozycję. Pomimo znacznie większej szybkości transmisji (maksymalnie 54 Mbit/s, realne są przepustowości rzędu 20 Mbit/s), standard 802.11a nie upowszechnił się, poza dużymi sieciami korporacyjnymi. Stosowana jest modulacja OFDM (ang. *Orthogonal Frequency-Division Multiplexing*, ortogonalne zwielokrotnianie w dziedzinie częstotliwości).

3.4. 802.11g

Opublikowanie w 2003 roku standardu 802.11g [22] było kolejnym powodem rynkowej porażki 802.11a. W rzeczywistości, 802.11g upowszechnił się jeszcze przed oficjalną ratyfikacją. Podobnie jak 802.11a, oferuje on szybkość 54 Mbit/s (realna przepustowość to około 20 Mbit/s) i działa w paśmie 2,4GHz (z modulacją OFDM). Istotną zaletą jest zachowanie zgodności wstecz z 802.11b, jednak w razie użycia starszych i nowszych urządzeń (tzn. standardu b i g) następuje znaczące spowolnienie działania całej sieci.

Oprócz wspomnianych już potencjalnych źródeł problemów z transmisją w paśmie 2,4GHz, kolejnym problemem, wynikającym z rosnącej popularności sieci bezprzewodowych, jest wzajemne zakłócanie się blisko położonych sieci, korzystających z tych samych lub sąsiednich kanałów radiowych. Problem ten dotyczy przede wszystkim dużych aglomeracji miejskich.

3.5. 802.11n

Prace nad standardem 802.11n [23] rozpoczęto w 2002 roku, a data zatwierdzenia standardu była wielokrotnie przekładana, aż do 2009 roku. Już wcześniej wiele firm rozpoczęło produkcję urządzeń zgodnych z propozycjami standardu, a Wi-Fi Alliance zajmowało się ich certyfikacją.

W 802.11n zastosowano technikę MIMO (ang. *Multiple Input Multiple Output*), w której jednocześnie wykorzystuje się wiele anten nadawczo-odbiorczych, by zwiększyć skuteczność transmisji. Odbierany może być sygnał docierający różnymi drogami, również w wyniku odbić. Możliwe jest uzyskanie szybkości transmisji na poziomie od 54 do 600 Mbit/s. Najwyższe szybkości uzyskuje się w razie skonfigurowania kanałów radiowych o podwójnej szerokości (40 MHz zamiast 20 MHz, jak we wcześniejszych implementacjach warstwy fizycznej 802.11). Jest to dozwolone zarówno w paśmie $5GHz$, jak też $2,4GHz$. W tym drugim przypadku istnieje jednak większe ryzyko wystąpienia zakłóceń między urządzeniami działającymi w tym samym paśmie, ponieważ dysponujemy tylko dwoma niekolidującymi kanałami (3 i 11).

Zasadniczo, standard 802.11n jest zgodny wstecz ze wszystkimi poprzednimi, tzn. 802.11a, b oraz g. Jednak umieszczenie starszych i nowszych urządzeń w tej samej sieci jest zawsze problematyczne i niekorzystnie wpływa na jej ogólną wydajność. W przypadku gdy w sieci muszą pracować karty sieciowe 802.11b/g, dobrym rozwiązaniem jest zastosowanie zaawansowanego punktu dostępowego z podwójnym modułem radiowym $2,4/5GHz$. Wówczas urządzenia 802.11b/g mogą być obsługiwane w paśmie $2,4GHz$, a urządzenia 802.11n – $5GHz$. Zakładamy tu, że posiadane urządzenia 802.11n mają możliwość pracy w paśmie $5GHz$, co nie musi mieć miejsca, ponieważ nie jest wymagane przez standard.

3.6. Przyszłość standardu

Prace grupy IEEE 802.11 nadal trwają. Najnowszy w chwili pisania tego podręcznika, zatwierdzony standard ma oznaczenie 802.11-2012 [16]. Włączono do niego szereg modyfikacji mechanizmów warstwy fizycznej i podwarstwy MAC, wprowadzanych w ciągu ostatnich lat. Obecnie powstaje standard IEEE 802.11ac, którego celem jest dalszy wzrost szybkości transmisji w lokalnych sieciach bezprzewodowych, do poziomu co najmniej 1 Gb/s, czyli zbliżonego do technologii Gigabit Ethernet. Będzie to możliwe w paśmie $5GHz$, przy wykorzystaniu technologii MIMO, szerszych kanałów i większej liczby strumieni.

Dysponowanie większą niż obecnie przepustowością sieci może umożliwić transmisję obrazu w jakości HD, synchronizację i tworzenie kopii zapasowych dużych plików, produkcję monitorów bezprzewodowych, zwiększenie skali wykorzystania Wi-Fi w automatyce przemysłowej.

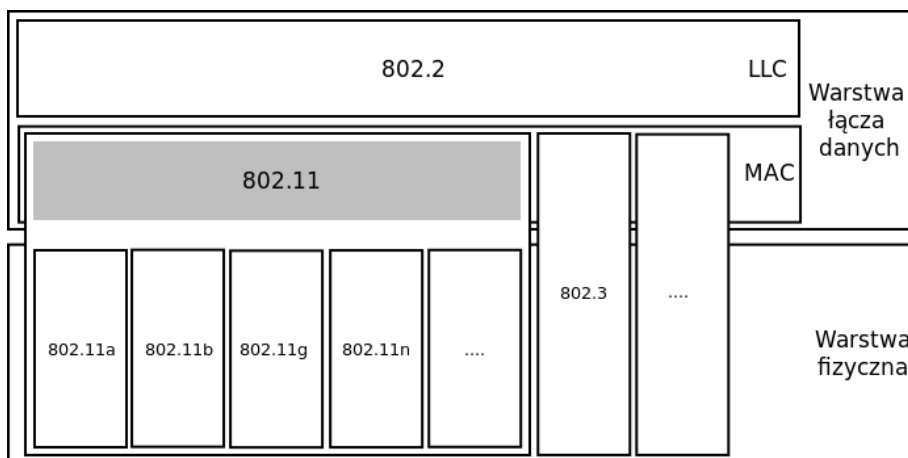
ROZDZIAŁ 4

MECHANIZM DOSTĘPU DO MEDIUM

4.1. Wstęp	28
4.2. Podstawy	28
4.3. Problem ukrytego węzła	30
4.4. RTS/CTS i fragmentacja ramek	31
4.5. Ramki 802.11	32

4.1. Wstęp

W początkowym etapie rozwoju lokalnych sieci bezprzewodowych, popularne było określanie ich mianem bezprzewodowego Ethernetu. Organizacja Wi-Fi Alliance, przyznająca urządzeniom certyfikaty zgodności z protokołami 802.11, jeszcze do 2002 roku nosiła nazwę Wireless Ethernet Compatibility Alliance (WECA). Rzeczywiście, w 802.11 [25] jest wiele podobieństw do metody dostępu do medium znanej z Ethernetu – CSMA/CD (IEEE 802.3 [24]). Jednak są również istotne różnice, które skłoniły do zaprzestania używania określenia “bezprzewodowy Ethernet”.



Rysunek 4.1. 802.11 w modelu ISO/OSI

Przedstawione w bieżącym rozdziale zagadnienia są związane z warstwą łącza danych modelu ISO/OSI, a dokładniej z podwarstwą MAC (szary prostokąt na rys. 4.1). Jest ona identyczna dla wszystkich obecnie wykorzystywanych wariantów lokalnych sieci bezprzewodowych, tzn. 802.11a, b, g oraz n (i najprawdopodobniej również przyszłych). Górna część warstwy łącza danych, czyli podwarstwa LLC, opisana standardem 802.2, jest wspólna dla 802.11, a także 802.3 (popularnie nazywanego Ethernetem) i innych technologii sieci LAN.

4.2. Podstawy

Rys. 4.2 przedstawia klasyczną sieć Ethernet, w której wszystkie hosty dołączone są do wspólnego medium – miedzianego kabla koncentrycznego. W danej chwili transmisję poprzez współdzielone medium może prowadzić tylko jedno urządzenie, a przesyłane dane docierają do wszystkich pozo-

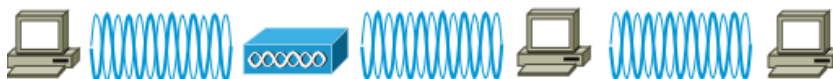
stałych. Urządzenia, które nie są adresatami wiadomości, powinny te dane zignorować, natomiast nie wolno im trwającej transmisji zakłócać. Jeżeli medium jest wolne, każde urządzenie może rozpocząć swoją transmisję w dowolnym momencie.



Rysunek 4.2. Klasyczny Ethernet CSMA/CD

W ten sposób może dojść do kolizji, tzn. sytuacji w której dwa urządzenia (lub więcej) stwierdzą, że medium jest dostępne i jednocześnie rozpoczną transmisję. Kolizja jest łatwa do wykrycia poprzez pomiar napięcia w kablu. Jeżeli stosowane jest nowsze medium – skrętka UTP, urządzenie dowiaduje się o kolizji rejestrując pojawienie się sygnału na parze przewodów służących do odbierania danych, podczas gdy prowadzi swoją transmisję przez drugą parę przewodów.

Kolizje są zjawiskiem normalnym. Standard 802.3 [24] określa protokół wielodostępu z badaniem stanu kanału i wykrywaniem kolizji (ang. *Carrier Sense Multiple Access with Collision Detection*, CSMA/CD). Zgodnie z nim, urządzenia, które spowodowały kolizję przerywają transmisję i emitują tzw. sygnał zagłuszania (ang. *jam signal*), by poinformować wszystkie węzły, że transmisja zakończyła się niepowodzeniem. Próbę transmisji mogą ponowić po upływie czasu zależnego od wartości wygenerowanej liczby pseudolosowej, na równych prawach z pozostałymi urządzeniami konkurującymi o dostęp do wspólnego medium. Mechanizm ten zmniejsza prawdopodobieństwo powtórnego wywołania kolizji przez te same urządzenia.



Rysunek 4.3. Sieć bezprzewodowa

W sieci z rys. 4.3, miedziany kabel został zastąpiony przez transmisję z wykorzystaniem fal radiowych. Wszystkie urządzenia wykorzystują ten sam kanał radiowy. Podobnie jak poprzednio, mamy do czynienia ze współdzielonym medium, poprzez które w danej chwili transmisję może prowadzić tylko jedno urządzenie, a dane docierają do wszystkich pozostałych. W związku z tym, podobnie jak w 802.3, zasadne wydaje się zaimplemen-

towanie mechanizmu wielodostępu z badaniem stanu kanału (ang. *Carrier Sense Multiple Access*, CSMA).

Problemem jest natomiast wykrywanie kolizji. Trudne jest zbudowanie urządzenia radiowego, które jest w stanie nadawać i jednocześnie nasłuchiwać na tym samym kanale, w celu wykrycia ewentualnej kolizji. Współczesne urządzenia sieciowe, zgodne z 802.11, takiej funkcji nie posiadają. Ponieważ nie ma możliwości bezpośredniego wykrycia kolizji, dostarczenie każdej ramki z danymi musi zostać potwierdzone informacją zwrotną – ramką ACK (*Acknowledgement*). Nieotrzymanie komunikatu ACK w ciągu określonego czasu skutkuje koniecznością retransmisji ramki, mimo że nie wiadomo, czy faktycznie poprzednio wysłana ramka nie dotarła do celu, czy też zakłócona została transmisja ramki ACK. Przedstawiony tu sposób działania jest głównym powodem tego, że przepustowość, jaką oferują sieci bezprzewodowe jest o około 50% niższa od teoretycznej szerokości pasma.

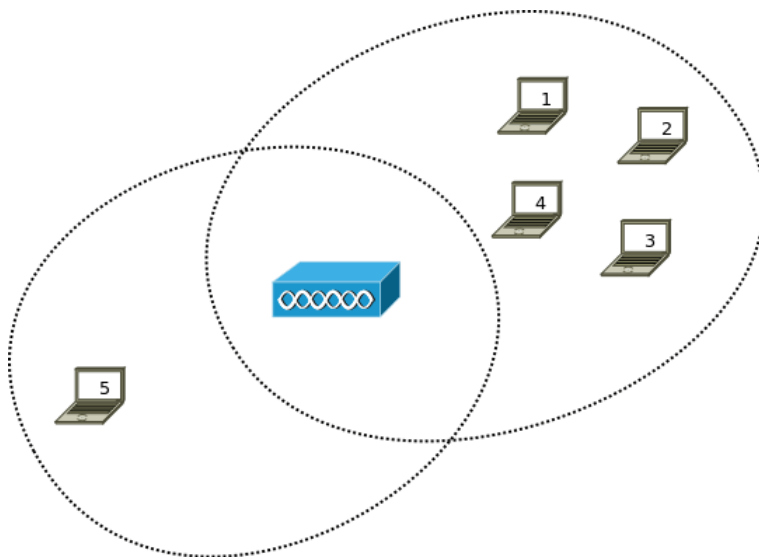
Kolizje w sieci bezprzewodowej skutkują znacznie większą degradacją ruchu sieciowego niż w technologii Ethernet. Dlatego zaimplementowano dodatkowe mechanizmy, które mają na celu zmniejszenie częstości ich występowania. Pełna nazwa mechanizmu dostępu do medium zdefiniowana w 802.11 to wielodostęp z badaniem stanu kanału i unikaniem kolizji (ang. *Carrier Sense Multiple Access with Collision Avoidance*, CSMA/CA).

Jednym z ważniejszych elementów protokołu dostępu do medium, związanych z unikaniem kolizji, jest rozproszona funkcja koordynacji (ang. *Distributed Coordination Function*, DCF) [25]. Jeżeli urządzenie chcące wysłać ramkę stwierdza, że medium jest dostępne, może natychmiast rozpocząć transmisję. W przeciwnym razie, należy poczekać do zakończenia trwającej transmisji, a następnie jeszcze przez dodatkowy czas zależny od wygenerowanej liczby pseudolosowej. Czas ten zmniejsza ryzyko wystąpienia kolizji w sytuacji gdy na dostępność medium może jednocześnie oczekiwać wiele hostów.

4.3. Problem ukrytego węzła

W sieci z rys. 4.4 komputery nr 1-4 znajdują się w zasięgu bezprzewodowego punktu dostępowego, jak również siebie nawzajem. Komputer nr 5 jest w zasięgu punktu dostępowego, jednak nie docierają do niego ramki wysyłane przez komputery 1-4. W tej sytuacji, transmisja ramek od komputerów 1-4 do punktu dostępowego może być często zakłócana przez komputer nr 5. Przedstawiona sytuacja jest określana mianem problemu ukrytego węzła (ang. *hidden node problem*).

Zjawisko to jest bardzo niekorzystne i znacząco obniża wydajność sieci. Może również nie być łatwe do wykrycia. Pośrednio o możliwości wystę-



Rysunek 4.4. Problem ukrytego węzła w sieci

powania ukrytego węzła może świadczyć informacja o dużej liczbie błędów transmisji, zarejestrowana w logach punktu dostępowego. Należy podjąć próbę wyeliminowania problemu poprzez przemieszczenie problematycznego węzła, usunięcie przeszkód dla fal radiowych, zmianę orientacji lub rodzaju anteny. Jeżeli nie jest to możliwe, należy skorzystać z dodatkowych mechanizmów: RTS/CTS oraz fragmentacji ramek.

4.4. RTS/CTS i fragmentacja ramek

Sprawdzanie stanu medium transmisyjnego (*Carrier Sense*) może odbywać się przy wykorzystaniu metod czysto fizycznych (nasłuch na danym kanale radiowym). Nie są one jednak wystarczające np. w sytuacji gdy w sieci występuje ukryty węzeł (rys. 4.4), do którego nie dociera sygnał radiowy z innych rejonów sieci. Należy wówczas skorzystać z tzw. wirtualnych metod sprawdzania stanu kanału. Jedną z nich jest użycie procedury RTS/CTS (*Request to Send / Clear to Send*).

Host, mając dane do wysłania, najpierw wysyła ramkę RTS – prośbę o zarezerwowanie medium na czas potrzebny na przesłanie ramki z danymi i potwierdzenia jej dostarczenia. Urządzenie, które ją odbierze (zwykle punkt dostępowy) staje się wtedy odpowiedzialne za proces rezerwacji medium. Ramka CTS, wysyłana w odpowiedzi na RTS, oznacza zgodę na rozpoczęcie żądanej uprzednio transmisji. Pozostałe urządzenia, dysponu-

jąc informacją o czasie, na jaki zostało zarezerwowane medium, nie będą tej transmisji zakłócać. Same ramki RTS/CTS również mogą ulegać kolizjom, ale ze względu na ich niewielki rozmiar nie powinno to stanowić istotnego problemu.

Użycie mechanizmu RTS/CTS skutkuje generowaniem dodatkowego ruchu w sieci, więc nie zawsze jest opłacalne, zwłaszcza w przypadku ramek z danymi o małym rozmiarze. Na poszczególnych węzłach sieci można skonfigurować wartość progową (*dot11RTSThreshold*), określającą rozmiar ramki, powyżej którego będzie stosowany RTS/CTS.

W przypadku transmisji ramek o dużej długości, ryzyko ich utraty, np. z powodu kolizji, jest znacznie większe niż dla małych ramek. Jeżeli w sieci często występują błędy, włączenie mechanizmu fragmentacji ramek może poprawić jej działanie. Ramki o długości większej od zdefiniowanego progu (*dot11FragmentationThreshold*) są zastępowane kilkoma mniejszymi. Urządzenie odbierające takie ramki jest odpowiedzialne za defragmentację. Fragmentacja wiąże się z dodatkowym narzutem, więc jej uruchomienie w poprawnie działającej sieci może dać efekt odwrotny od zamierzonego.

Mechanizmy RTS/CTS i fragmentacji często stosowane są łącznie, w celu zredukowania negatywnego wpływu ukrytych węzłów na działanie sieci. Dobór optymalnych parametrów wymaga jednak doświadczenia. Lepszym rozwiązaniem jest zawsze zlokalizowanie i usunięcie źródła problemu.

4.5. Ramki 802.11

Standard 802.11 [25] przewiduje użycie trzech typów ramek: zarządzających (*management*), kontrolnych (*control*) i do transmisji danych (*data*). W obrębie każdego typu wyróżnia się szereg podtypów. W ramce można wyodrębnić nagłówek MAC, ciało ramki (o zmiennej długości) i sekwencję kontrolną (32-bitową CRC) – rys. 4.5.

Frame Control 2B	Duration /ID 2B	Address 1 6B	Address 2 6B	Address 3 6B	Sequence Control 2B	Address 4 6B	QoS Control 2B	HT Control 4B	Frame Body 0 - 7951B	FCS 4B
Protocol Version 2b	Type 2b	Subtype 4b	To DS 1b	From DS 1b	More fragments 1b	Retry 1b	Power Management 1b	More Data 1b	Protected Frame 1b	Order 1b

Rysunek 4.5. Format ramki 802.11 [25]

Ramka 802.11 zdecydowanie różni się od ramki Ethernet (zarówno Ethernet II, jak i IEEE 802.3). Identyczne są 48-bitowe adresy MAC, jednak występują aż cztery pola adresowe. Poniżej przedstawiono informacje o przeznaczeniu poszczególnych pól:

- *Protocol Version* służy do oznaczenia wersji standardu. Obecnie jest to “0”. Kolejne wartości będą użyte w razie wprowadzenia do standardu istotnych zmian, uniemożliwiających zachowanie zgodności ze starszymi wersjami.
- *Type, Subtype* identyfikuje typ ramki (kontrolna, zarządzająca, przesyłająca dane) i podtyp.
- *To DS, From DS* określają sposób postępowania z ramką. Znaczenie poszczególnych kombinacji przedstawia poniższa tabela.

Tabela 4.1. Znaczenie poszczególnych wartości pól To DS i From DS

To DS	From DS	Znaczenie
0	0	ramka przekazywana bezpośrednio między hostami w sieci IBSS, ramki kontrolne i zarządzające
1	0	ramka przekazywana przez hosta w sieci bezprzewodowej do punktu dostępowego, przeznaczona do przesłania do systemu dystrybucyjnego lub innego hosta połączonego z tym samym punktem dostępowym
0	1	ramka przekazywana przez punkt dostępowy do hosta w sieci bezprzewodowej, pochodząca z systemu dystrybucyjnego lub od innego hosta z tego samego BSS
1	1	wykorzystywane w przypadku bezprzewodowego systemu dystrybucyjnego, np. w sieci z mostami bezprzewodowymi

- *More Fragments* – wartość “1” oznacza, że ramka powstała w wyniku fragmentacji większej ramki.
- *Retry* otrzymuje wartość “1” w przypadku powtórnej transmisji ramki. Ułatwia urządzeniu odbierającemu eliminowanie duplikatów ramek.
- *Power Management* informuje o stanie oszczędzania energii (“1”) lub stanie aktywnym (“0”) danego urządzenia.
- *More Data* informuje hosta w stanie oszczędzania energii o tym, że punkt dostępowy nadal posiada w buforze przeznaczone dla niego dane.
- *Protected Frame* informuje o zaszyfrowaniu danych przesyłanych w ramce.

- *Order* – wartość “1” wymusza przetwarzanie ramek w ustalonej kolejności (obecnie zazwyczaj “0”).
- *Duration/ID* – w zależności od typu ramki, zawiera identyfikator stacji nadawczej, wyrażony w milisekundach czas potrzebny na transmisję lub ustaloną wartość.
- Cztery pola adresowe (*Address*) są wykorzystywane w różny sposób, w zależności od sytuacji. Dalej przedstawionych jest kilka przykładów.
- *Sequence Control* ma zastosowanie przy fragmentacji ramek.
- *QoS Control* zawiera różne parametry związane z jakością usług.
- *HT Control* jest wykorzystywane przez niektóre ramki kontrolne i zarządzające.
- *Frame Body* – “ładunek”, w zależności od typu ramki. W przypadku ramki transmitującej dane, jest to pakiet IP, opakowany w ramkę LLC (802.2).
- *FCS* – sekwencja kontrolna.

Rys. 4.6 przedstawia sieć, na przykładzie której zostanie przedstawiony sposób wykorzystania pól adresowych w ramce 802.11. 1111–6666 są uproszczonymi adresami MAC hostów, natomiast aaaa i bbbb – adresami MAC interfejsów radiowych punktów dostępowych (tzw. *Basic Service Set Identifier*, BSSID).

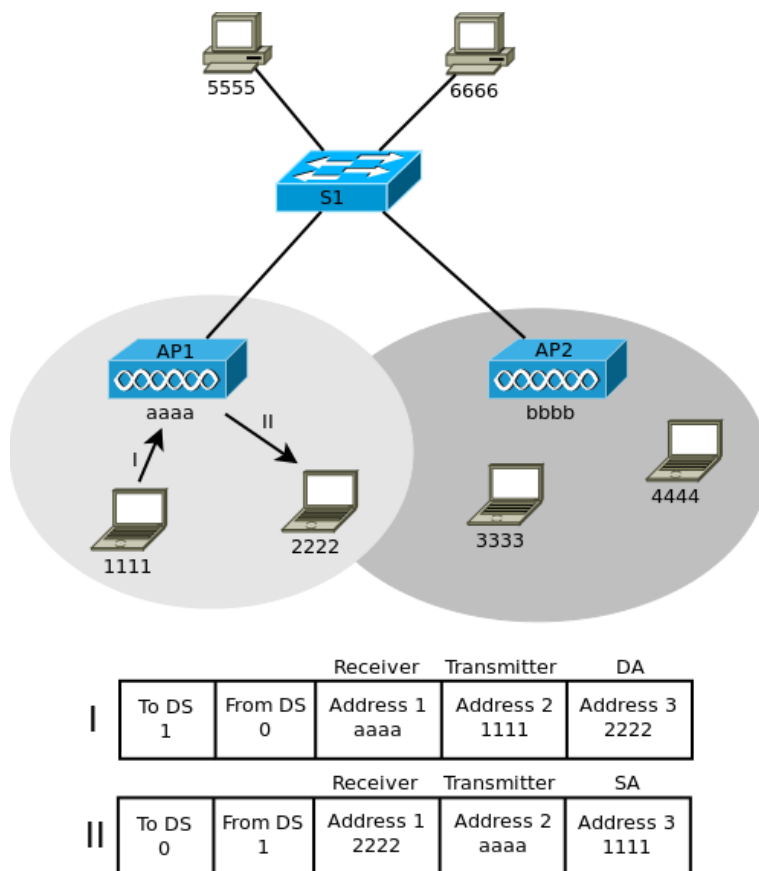
Przewodowa sieć Ethernet, z przełącznikiem S1, stanowi tu system dystrybucyjny (*Distribution System*, DS), łączący poszczególne punkty dostępowe i przewodową sieć lokalną. Jest to najczęstsze rozwiązanie, chociaż standard 802.11 nie określa sposobu realizacji systemu dystrybucyjnego. Może on być również bezprzewodowy.

W ramce 802.11 (rys. 4.5) adres 1 jest adresem odbiorcy (*receiver address*), tzn. urządzenia, które otrzymuje ramkę, ale niekoniecznie jest jej miejscem docelowym. Adres 2 to adres transmitera (*transmitter address*), czyli urządzenia wysyłającego ramkę, ale niekoniecznie będącego jej początkowym źródłem. Adres 3 to adres źródłowy (SA) lub docelowy (DA), w sieci bezprzewodowej lub Ethernet, lub BSSID, w zależności od sytuacji. Adres 4 ma zastosowanie w przypadku bezprzewodowego systemu dystrybucyjnego i nie będzie wykorzystywany w prezentowanych tu przykładach.

Załóżmy, że host 1111 wysyła ramkę przeznaczoną dla hosta 2222. Transmisja zostanie zrealizowana w następujący sposób:

- Ramka I (rys. 4.6) jest przesyłana przez hosta 1111 do punktu dostępowego AP1.
- Punkt dostępowy przesyła ramkę II do hosta docelowego (2222).

Należy tu zwrócić uwagę, że w przeciwieństwie do przełącznika Ethernet, realizującego przełączanie przezroczyste (ang. *transparent switching*), punkt dostępowy modyfikuje zawartość nagłówka ramek, które przekazu-

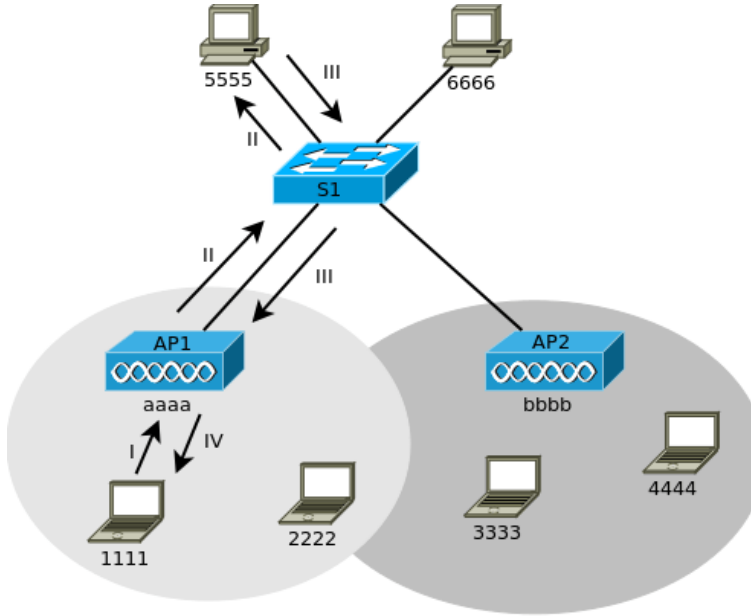


Rysunek 4.6. Przekazywanie ramek w sieci z punktem dostępowym

je (rys. 4.6). Ponadto, istotną rolę pełni adres MAC interfejsu radiowego punktu dostępowego (BSSID). W przypadku przełącznika Ethernet, jest on potrzebny jedynie w razie zdalnego zarządzania urządzeniem. Nie ma natomiast żadnego znaczenia w kontekście roli, jaką urządzenie pełni w sieci.

Kolejny przykład (rys. 4.7) ilustruje komunikację między siecią bezprzewodową a przewodową (Ethernet):

- Ramka I wysyłana przez hosta 1111, przeznaczona dla hosta 5555, ma identyczny układ, jak w poprzednim przykładzie (lecz z innym adresem docelowym).
- Punkt dostępowy musi dokonać translacji ramki 802.11 na ramkę Ethernet (ramka II). Następnie przekazuje ją do systemu dystrybucyjnego w celu dostarczenia do adresata.
- W przypadku przesyłania ramki z sieci Ethernet do sieci bezprzewo-



	Receiver		Transmitter		DA
I	To DS 1	From DS 0	Address 1 aaaa	Address 2 1111	Address 3 5555
II	Destination Address 5555		Source Address 1111		
III	Destination Address 1111		Source Address 5555		
	Receiver		Transmitter		SA
IV	To DS 0	From DS 1	Address 1 1111	Address 2 aaaa	Address 3 5555

Rysunek 4.7. Przekazywanie ramek między siecią bezprzewodową i Ethernet

dowej, punkt dostępowy dokonuje translacji ramki Ethernet (ramka III) na ramkę 802.11 (ramka IV).

Punkt dostępowy zna adresy MAC urządzeń, z którymi jest połączony bezprzewodowo, już od etapu asocjacji, i przechowuje je w odpowiedniej tablicy. Jeżeli otrzymuje ramkę przeznaczoną dla nieznanego urządzenia, wówczas dokonuje odpowiedniej translacji i przekazuje ją do sieci Ethernet. Przełącznik Ethernet traktuje adresy MAC urządzeń z sieci bezprze-

wodowej identycznie jak adresy urządzeń z sieci Ethernet, umieszczając je w swojej tablicy adresów MAC.

Dla hosta wysyłającego ramkę nie ma znaczenia to, czy jej adresat znajduje się w sieci przewodowej czy bezprzewodowej. Podobnie, host odbierający ramkę nie otrzymuje informacji o tym, czy host źródłowy jest w sieci przewodowej czy bezprzewodowej.

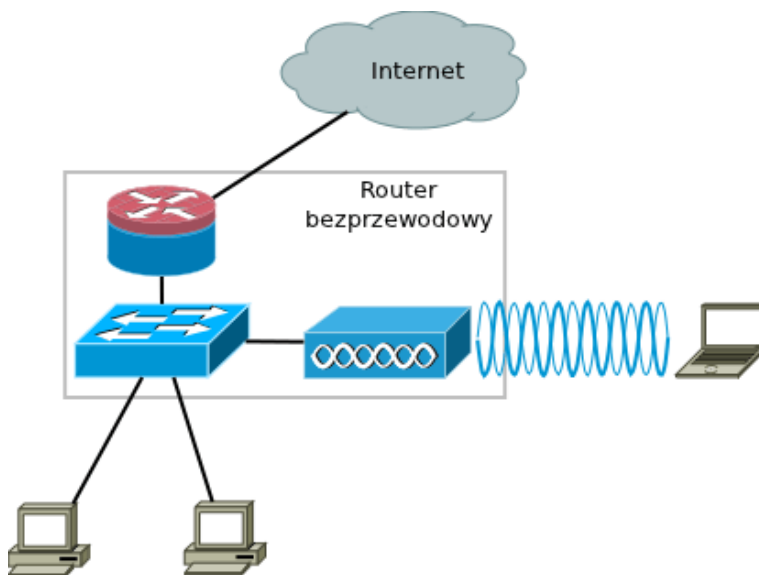
ROZDZIAŁ 5

BEZPRZEWODOWE PUNKTY DOSTĘPowe

5.1.	Wstęp	40
5.2.	Konfiguracja punktu dostępowego Cisco Aironet	41
5.2.1.	Podstawy	41
5.2.2.	Przywracanie ustawień fabrycznych	41
5.2.3.	Konfiguracja poprzez przeglądarkę WWW	42
5.2.4.	Konfiguracja hosta	48
5.2.5.	Zadanie – konfiguracja poprzez przeglądarkę WWW	49
5.2.6.	Wskazówki do zadania 5.2.5	50
5.2.7.	Konfiguracja poprzez wiersz poleceń IOS	51
5.2.8.	Zadanie – konfiguracja poprzez wiersz poleceń IOS	53

5.1. Wstęp

Bezprzewodowe punkty dostępowe (ang. *access points*) są zasadniczym elementem sieci bezprzewodowej. Są to urządzenia pracujące w drugiej warstwie modelu ISO/OSI. W sieciach domowych częściej korzysta się z routerów bezprzewodowych. Jedno, niewielkie urządzenie pełni wówczas rolę routera z translacją adresów, serwera DHCP, firewalla, kilkuportowego przełącznika Ethernet i bezprzewodowego punktu dostępowego (rys. 5.1). Routery bezprzewodowe są łatwe do skonfigurowania, dzięki przyjaznemu interfejsowi dostępnemu przez przeglądarkę WWW, jednak liczba opcji konfiguracyjnych jest zwykle mocno ograniczona.



Rysunek 5.1. Schemat logiczny routera bezprzewodowego

Oprócz autonomicznych punktów dostępowych, których konfiguracji poświęcona jest większość bieżącego rozdziału, występują również karty rozszerzeń, które można instalować w urządzeniach o budowie modułowej. Kolejną grupę stanowią tzw. lekkie punkty dostępowe (ang. *lightweight access point*). Do pracy wymagają one połączenia z kontrolerem sieci bezprzewodowej, który jednocześnie może zarządzać wieloma punktami dostępowymi, a wszelkie operacje konfiguracyjne są wykonywane za jego pośrednictwem. To rozwiązanie jest stosowane w dużych sieciach korporacyjnych. Zarządzanie siecią zawierającą wiele autonomicznych punktów dostępowych byłoby znacznie trudniejsze. Więcej na ten temat można znaleźć w Rozdziale 9.

5.2. Konfiguracja punktu dostępowego Cisco Aironet

5.2.1. Podstawy

Początkową konfigurację punktu dostępowego Cisco Aironet można przeprowadzić używając wiersza poleceń IOS, poprzez połączenie konsolowe, lub korzystając z interfejsu graficznego dostępnego dla przeglądarki WWW, poprzez połączenie Ethernet (rys. 5.2). Zakładamy tu, że skonfigurowanym urządzeniem jest punkt dostępowy Cisco Aironet serii 1200 (oznaczenie modelu: AIR-AP1231G-E-K9), z zainstalowanym systemem operacyjnym IOS w wersji 12.3(8). W przypadku innych wersji, mogą wystąpić różnice dotyczące pewnych szczegółów. Przykładowo, w starszych urządzeniach Aironet, interfejs radiowy był domyślnie włączony, z działającym SSID *tsunami*, z otwartym uwierzytelnianiem. Natychmiast po włączeniu nowego urządzenia, było ono gotowe do pracy. Była więc możliwość zdalnego zalogowania się z prawami administratora, przy użyciu standardowego hasła i loginu. Jeżeli ustawienia te nie zostały zmienione, np. wskutek nieświadomości administratora, sieć była narażona na przeprowadzenie bardzo prostego ataku oraz nieuprawnione korzystanie z jej zasobów. Współczesne urządzenia nie posiadają domyślnej konfiguracji SSID, a interfejs radiowy jest wyłączony.



Rysunek 5.2. Bezprzewodowy punkt dostępowy z widocznymi gniazdami przyłączeniowymi

5.2.2. Przywracanie ustawień fabrycznych

Jeżeli urządzenie jest wyposażone w przycisk *Mode* (rys. 5.2), w celu przywrócenia ustawień fabrycznych należy odłączyć zasilanie (o ile jest włączone), wcisnąć i przytrzymać przycisk, włączyć zasilanie, a następnie zwolnić przycisk, gdy dioda statusu zmieni kolor na bursztynowy (po około

2 sekundach). W przypadku urządzeń pozbawionych przycisków, opisy odpowiednich procedur można znaleźć w dokumentacji [26]. Jeżeli natomiast dysponujemy już dostępem do trybu uprzywilejowanego IOS, można użyć typowych dla urządzeń Cisco poleceń:

```
erase startup-config
reload
```

Standardowe parametry portu konsolowego są takie same jak w innych urządzeniach Cisco, tzn.:

- 9600 b/s,
- 8 bitów danych,
- brak parzystości,
- 1 bit stopu,
- brak kontroli przepływu.

Domyślnym hasłem dostępu do trybu uprzywilejowanego jest *Cisco*. W razie zdalnego logowania do urządzenia, należy użyć nazwy użytkownika *Cisco* i hasła *Cisco*. Hasła te należy niezwłocznie zmienić, ponieważ ich pozostawienie stanowi poważną lukę w systemie bezpieczeństwa.

Jeżeli punkt dostępowy jest dołączony do lokalnej sieci Ethernet, będzie próbował uzyskać adres IP od serwera DHCP. Jeżeli się to powiedzie, będzie można połączyć się z punktem dostępowym poprzez telnet (wiersz poleceń IOS) lub HTTP (interfejs graficzny). Niektóre wersje urządzeń mają z kolei skonfigurowany statycznie domyślny adres IP: 10.0.0.1.

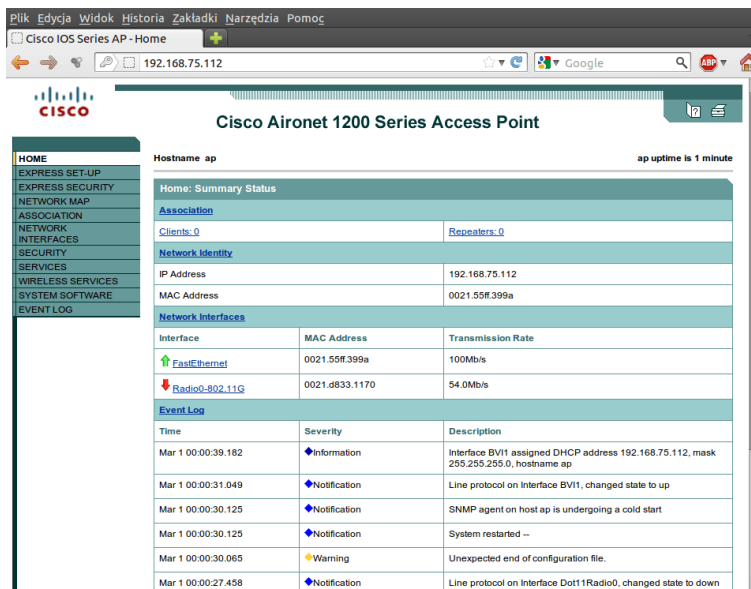
Jeżeli zamierzamy skonfigurować punkt dostępowy poprzez przeglądarkę WWW, ale nie możemy nawiązać z nim połączenia sieciowego (bo np. nie dysponujemy serwerem DHCP), podstawowe ustawienia protokołu IP należy wprowadzić przy użyciu połączenia konsolowego i wiersza poleceń. Następnie połączenie przeglądarką WWW powinno już być możliwe.

5.2.3. Konfiguracja poprzez przeglądarkę WWW

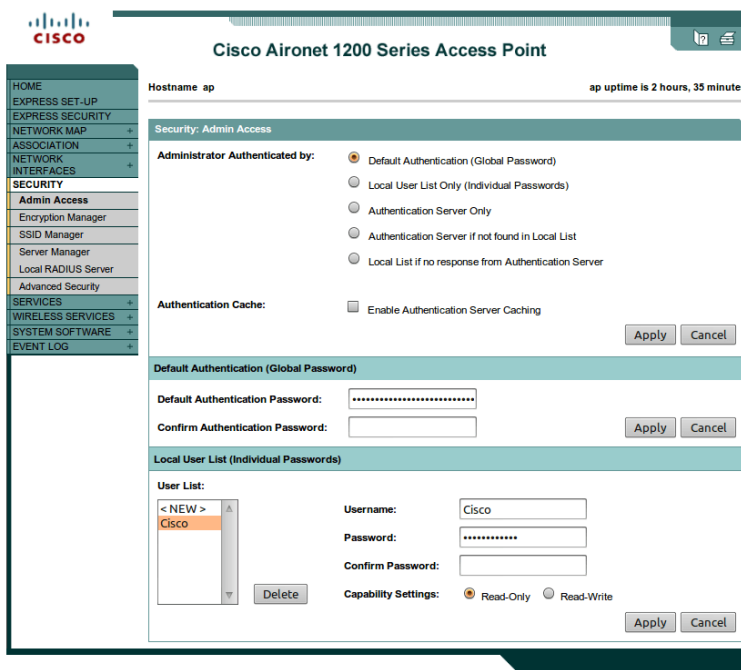
Jeżeli punkt dostępowy ma prawidłowy adres IP i można się z nim zdalnie połączyć przeglądarką WWW, po podaniu domyślnej nazwy użytkownika i hasła (*Cisco*), powinna ukazać się strona zbliżona do przedstawionej na rys. 5.3. Radio0-802.11G jest interfejsem bezprzewodowym, który obecnie jest wyłączony.

Poniżej informacji o interfejsach, w logu zdarzeń systemowych (*Event Log*) widnieje informacja o uzyskaniu adresu IP od serwera DHCP:

```
Interface BVI1 assigned DHCP address 192.168.75.112,
mask 255.255.255.0, hostname ap
```



Rysunek 5.3. Główny ekran interfejsu graficznego punktu dostępowego



Rysunek 5.4. Ekran konfiguracji zabezpieczeń dostępu do urządzenia

Adres IP nie jest przypisywany bezpośrednio interfejsowi FastEthernet ani bezprzewodowemu, lecz wirtualnemu interfejsowi BV11 (*Bridge Virtual Interface*). Można połączyć się z nim poprzez dowolny spośród interfejsów fizycznych.

Ze względów bezpieczeństwa, konfigurowanie punktu dostępowego powinno się rozpocząć od zmiany domyślnych haseł. Można to zrobić korzystając z ekranu *Admin Access* w sekcji *Security* – rys. 5.4. Należy zmienić hasło trybu uprzywilejowanego (*Default Authentication Password*), w sekcji *Local User List* stworzyć własne konto administratora i usunąć użytkownika *Cisco*. Po wprowadzeniu jakichkolwiek modyfikacji, konieczne jest ich zatwierdzenie poprzez kliknięcie przycisku *Apply*.

The screenshot shows the Cisco Aironet 1200 Series Access Point configuration interface. The main section is titled "Express Set-Up" and contains the following fields and options:

- Host Name:** Input field containing "ap".
- MAC Address:** Input field containing "0021.55ff.399a".
- Configuration Server Protocol:** Radio buttons for "DHCP" (selected) and "Static IP".
- IP Address:** Input field containing "192.168.75.112".
- IP Subnet Mask:** Input field containing "255.255.255.0".
- Default Gateway:** Input field containing "192.168.75.1".
- SNMP Community:** Input field containing "defaultCommunity".
- SNMP Access:** Radio buttons for "Read-Only" (selected) and "Read-Write".
- Radio0-802.11G:**
 - Role in Radio Network:** Radio buttons for "Access Point" (selected), "Repeater", "Root Bridge", "Non-Root Bridge", "Workgroup Bridge", and "Scanner".
 - Optimize Radio Network for:** Radio buttons for "Throughput", "Range", "Default" (selected), and "Custom".
 - Arlonet Extensions:** Radio buttons for "Enable" (selected) and "Disable".

At the bottom right, there are "Apply" and "Cancel" buttons. The top right corner shows "ap uptime is 1 hour, 37 minutes".

Rysunek 5.5. Podstawowe ustawienia – *Express Setup*

Rys. 5.5 przedstawia ekran podstawowej konfiguracji (*Express Setup*), umożliwiającą między innymi:

- nadanie nazwy urządzeniu (odpowiednik polecenia *hostname*),
- skonfigurowanie adresu IP (statycznie lub poprzez pobranie z serwera DHCP),
- określenie roli urządzenia w sieci bezprzewodowej (domyślnie *Access Point* – punkt dostępowy).

The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point" and the host name is "ap". The uptime is "2 hours, 1 minute". The left sidebar contains navigation options: HOME, EXPRESS SET-UP, EXPRESS SECURITY (highlighted), NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG.

The main content area is titled "Express Security Set-Up" and "SSID Configuration". It contains three sections:

- 1. SSID:** A text input field for the SSID name and a checkbox for "Broadcast SSID in Beacon".
- 2. VLAN:** Radio buttons for "No VLAN" (selected) and "Enable VLAN ID: [input] (1-4094)". A checkbox for "Native VLAN" is also present.
- 3. Security:** Radio buttons for "No Security" (selected), "Static WEP Key", "EAP Authentication", and "WPA".
 - Under "Static WEP Key": A "Key 1" dropdown, a text input field, and a "128 bit" dropdown.
 - Under "EAP Authentication": Two sets of "RADIUS Server" (text input) and "RADIUS Server Secret" (text input) fields.
 - Under "WPA": Two sets of "RADIUS Server" (text input) and "RADIUS Server Secret" (text input) fields.

At the bottom right of the configuration area are "Apply" and "Cancel" buttons.

Below the configuration area is an "SSID Table" with the following data:

Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
<input type="radio"/>	Lab1	none	none	open	none		<input checked="" type="checkbox"/>

Rysunek 5.6. Ustawienia SSID – ekran *Express Security*

Ekran *Express Security* (rys. 5.6) umożliwia stworzenie nowego lub usunięcie istniejącego identyfikatora SSID. W tym celu w polu *1. SSID* należy wprowadzić dowolnie wybraną nazwę SSID, zaznaczyć pole *Broadcast SSID in Beacon* w celu włączenia rozgłaszania informacji o SSID (zagadnienie jest dokładniej wyjaśnione w Rozdziale 6., dotyczącym bezpieczeństwa), a następnie kliknąć *Apply*. Po chwili informacja o stworzonym SSID (w przykładzie z rysunku – *Lab1*) powinna pojawić się w tabelce na dole ekranu.

Prezentowany tu punkt dostępowy, w przeciwieństwie do prostych urządzeń amatorskich, może jednocześnie obsługiwać wiele SSID, z różnymi ustawieniami, widzianych przez użytkowników jako odrębne sieci bezprzewodowe. Jednak tylko w przypadku jednej z nich, opcja *Broadcast SSID in Beacon* może być włączona.

Ostatnią spośród podstawowych czynności konfiguracyjnych jest włączenie interfejsu bezprzewodowego. Na głównej stronie urządzenia należy

Cisco Aironet 1200 Series Access Point

HOME | EXPRESS SET-UP | EXPRESS SECURITY | NETWORK MAP | ASSOCIATION | NETWORK INTERFACES | IP Address | FastEthernet | **Radio0-802.11G** | Radio1-not installed | SECURITY | SERVICES | WIRELESS SERVICES | SYSTEM SOFTWARE | EVENT LOG

RADIO0-802.11G STATUS | DETAILED STATUS | SETTINGS | CARRIER BUSY TEST

Hostname **ap** | ap uptime is 2 hours, 23 minutes

Network Interfaces: Radio0-802.11G Status

Configuration			
Software Status	Disabled ↓	Hardware Status	Down ↓
Operational Rates	1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0 Mb/sec	Basic Rate	1.0, 2.0, 5.5, 11.0 Mb/sec
Aironet Extensions	Enabled	Carrier Set	EMEA
Current Radio Channel	0 MHz Channel 0	Transmitter Power CCK/OFDM	50 mW / 30 mW
Role in Network	Access Point		
Interface Statistics			
Interface Resets	0		
Receive / Transmit Statistics			
Receive		Transmit	
5 Min Input Rate (bits/sec)	0	5 Min Output Rate (bits/sec)	0
5 Min Input Rate (packets/sec)	0	5 Min Output Rate (packets/sec)	0
Time Since Last Input	never	Time Since Last Output	never
Total Packets Input	0	Total Packets Output	0
Total Bytes Input	0	Total Bytes Output	0
Error Statistics			
Receive		Transmit	
Total Input Errors	0	Total Output Errors	0
Throttles	0	Last Output Hang	never

Clear Refresh

Rysunek 5.7. Ekran interfejsów sieciowych

wybrać sekcję *Network Interfaces*, a następnie interfejs, który ma zostać uruchomiony (np. *Radio0-802.11G*) – rys. 5.7. W zakładce *Settings* (rys. 5.8) można skonfigurować szereg parametrów interfejsu. Aby włączyć go, pozostawiając domyślne wartości, wystarczy zaznaczyć opcję *Enable* i kliknąć *Apply*. Istotną kwestią jest wybranie odpowiedniego kanału radiowego (*Default Radio Channel*). W razie pozostawienia domyślnej opcji (*Least-Congested Frequency*), interfejs zostanie uruchomiony po trwającym kilkadziesiąt sekund skanowaniu, w celu automatycznego znalezienia najmniej zakłócanego kanału. O działaniu interfejsu poinformują dwie zielone (zamiast czerwonych) strzałki w oknie z rys. 5.8. Pozostałe opcje konfiguracyjne dotyczą między innymi:

- roli urządzenia w sieci,
- obsługiwanych przepustowości,
- mocy nadajnika,
- sposobu korzystania z anten (co jest istotne w przypadku urządzeń umożliwiających dołączenie więcej niż z jednej anteny),
- fragmentacji ramek i mechanizmu RTS/CTS.

Jeżeli konfiguracja interfejsu przebiegła poprawnie, sieć bezprzewodowa

The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point. The main content area is titled 'Network Interfaces: Radio0-802.11G Settings'. It includes the following configuration options:

- Enable Radio:** Enable Disable
- Current Status (Software/Hardware):** Disabled ↓ Down ↓
- Role in Radio Network:**
 - Access Point
 - Access Point (Fallback to Radio Shutdown)
 - Access Point (Fallback to Repeater)
 - Repeater
 - Root Bridge
 - Non-Root Bridge
 - Root Bridge with Wireless Clients
 - Non-Root Bridge with Wireless Clients
 - Workgroup Bridge
 - Scanner
- Data Rates:**
 - Best Range | Best Throughput | Default
 - 1.0Mb/sec: Require Enable Disable
 - 2.0Mb/sec: Require Enable Disable
 - 5.5Mb/sec: Require Enable Disable
 - * 6.0Mb/sec: Require Enable Disable

Rysunek 5.8. Konfiguracja interfejsu radiowego

The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point, specifically the 'Association' section. It includes the following information:

- Association:** Clients: 2, Repeaters: 0
- View:** Client Repeater (with an 'Apply' button)
- Radio0-802.11G:**
 - SSID Lab1:**

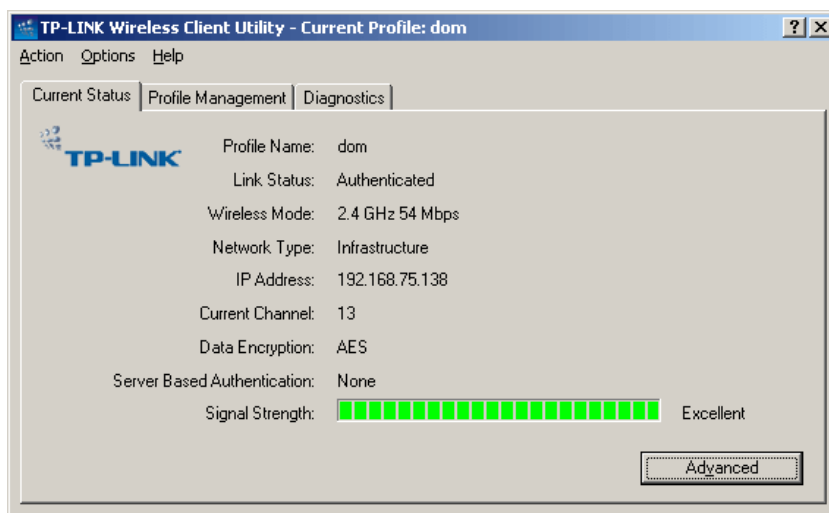
Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
ccx-client	DESKTOP	192.168.75.138	0014.7810.74f4	Associated	self	none
unknown	NONE	192.168.75.140	78e4.003f.24e9	Associated	self	none

Rysunek 5.9. Informacja o klientach dołączonych do punktu dostępowego

z wybranym SSID powinna zostać wykryta przez hosty wyposażone w bezprzewodowe karty sieciowe i powinno być możliwe połączenie z nią (asocjacja). Informacja o hostach aktualnie dołączonych do punktu dostępowego jest dostępna w sekcji *Association* – rys. 5.9.

W tym miejscu należy zauważyć, że skonfigurowany w powyższy sposób punkt dostępowy jest “otwarty” i nie przeprowadza żadnej weryfikacji urządzeń, które się z nim łączą. Tego typu konfiguracja bywa obecnie stosowana tylko w przypadku hotspotów, czyli punktów dostępowych zapewniających wszystkim chętnym dostęp do Internetu w różnego rodzaju miejscach użyteczności publicznej. Wszelkie inne sieci powinny być wyposażone w mechanizmy bezpieczeństwa adekwatne do ich przeznaczenia. Jednak przed ich uruchomieniem, w celu łatwiejszego wykrycia ewentualnych błędów, wskazane jest, by najpierw przetestować działanie sieci otwartej (zachowując ostrożność, by nie udostępnić zasobów nieuprawnionym użytkownikom). Zalecenie to odnosi się także do ćwiczeń laboratoryjnych w kolejnych rozdziałach.

5.2.4. Konfiguracja hosta



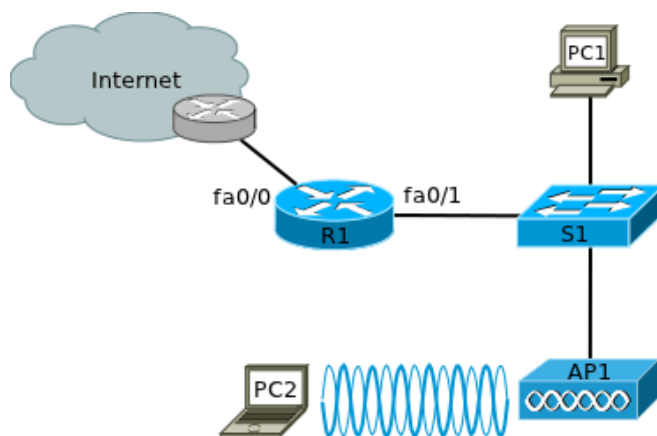
Rysunek 5.10. Narzędzie konfiguracyjne bezprzewodowej karty sieciowej

Aby było możliwe połączenie hosta z siecią bezprzewodową, niezbędne jest odpowiednie oprogramowanie: sterownik karty sieciowej i interfejs umożliwiający skonfigurowanie podstawowych parametrów (w wariantach minimalistycznym – tylko SSID). Często użytkownik może wybrać oprogramowanie dostarczone wraz z systemem operacyjnym lub znacznie bardziej rozbudowane narzędzia oferowane przez producenta karty sieciowej (rys. 5.10).

Ustawienia IP (adres, maskę podsieci, adres bramy domyślnej i serwera DNS) można skonfigurować identycznie jak w przypadku sieci przewodowej.

wej, tzn. statycznie lub wykorzystując serwer DHCP (o ile jest dostępny). W praktyce, konfiguracja statyczna jest obecnie rzadko stosowana.

5.2.5. Zadanie – konfiguracja poprzez przeglądarkę WWW



Rysunek 5.11. Schemat topologii logicznej sieci

1. Połącz urządzenia zgodnie z powyższym schematem (rys. 5.11). Jeżeli nie jest możliwe połączenie routera z Internetem, w miejsce chmury podłącz komputer lub inne urządzenie symulujące takie połączenie.
2. Przeprowadź podstawową konfigurację routera (nazwa, hasła). Interfejs fa0/0 skonfiguruj w sposób umożliwiający połączenie z Internetem. W sieci lokalnej użyj adresów z puli 192.168.1.0/24. Pierwszy adres przypisz interfejsowi routera fa0/1.
3. Na routerze uruchom usługę serwera DHCP dla sieci lokalnej (dokładniejsze wskazówki zawiera Dodatek A.1). Jeżeli dostępny jest serwer DNS, spowoduj by informacja o jego adresie była również przekazywana klientom. Upewnij się, że komputer PC1 otrzymał prawidłowe ustawienia IP od serwera DHCP.
4. Na routerze skonfiguruj domyślną trasę statyczną prowadzącą do najbliższego routera w chmurze. Skonfiguruj mechanizm translacji adresów (przeciążony NAT) tak, by wszystkie hosty z sieci lokalnej mogły korzystać z Internetu (wskazówki zawiera Dodatek A.2). Przetestuj połączenie komputera PC1 z dowolnym hostem w Internecie.
5. Sprawdź jaki adres IP otrzymał punkt dostępowy (możesz użyć polecenia `show ip dhcp binding` na routerze lub połączyć się z konsolą punktu dostępowego). Na komputerze PC1 uruchom przeglądarkę WWW i połącz się z punktem dostępowym.

6. Skonfiguruj podstawowe zabezpieczenia punktu dostępowego, dowolny SSID (z opcją rozgłaszania) i interfejs radiowy. Analizując wyświetlane informacje upewnij się, że interfejs radiowy został włączony.
7. Skonfiguruj komputer PC2 tak, aby mógł połączyć się z siecią bezprzewodową. PC2 powinien otrzymać adres IP oraz pozostałe ustawienia od serwera DHCP działającego na routerze i mieć możliwość łączenia się z pozostałymi urządzeniami w sieci lokalnej oraz w Internecie. Po wykonaniu zadania punkt dostępowy należy wyłączyć, ponieważ funkcjonuje on jako publicznie dostępny hotspot.

5.2.6. Wskazówki do zadania 5.2.5

Listing 5.1. Istotne fragmenty pliku konfiguracyjnego routera R1

```

[ ... ]
 2 service password-encryption
  !
 4 hostname R1
  !
 6 enable secret 5 x1xmERrxhx5rVt7rPNoS4wqbXKX7m0
  !
 8 ip dhcp excluded-address 192.168.1.1
  !
10 ip dhcp pool PULA1
    network 192.168.1.0 255.255.255.0
12 default-router 192.168.1.1
    dns-server adres_serwera_dns
14 !
    interface FastEthernet0/0
16 ip address adres_maska | dhcp
    ip nat outside
18 duplex auto
    speed auto
20 !
    interface FastEthernet0/1
22 ip address 192.168.1.1 255.255.255.0
    ip nat inside
24 duplex auto
    speed auto
26 !
    ip nat inside source list 1 interface FastEthernet0/0
28                                     overload
    ip classless
30 !
    access-list 1 permit 192.168.1.0 0.0.0.255
32 !
    line con 0
34 password 7 08294D5D0516524F4B
    login

```

```
36 line vty 0 4
    login
38 line vty 5 15
    login
40 !
    end
```

5.2.7. Konfiguracja poprzez wiersz poleceń IOS

Ogólne zasady konfigurowania bezprzewodowych punktów dostępowych są identyczne jak w przypadku innych urządzeń wyposażonych w system operacyjny IOS [4, 5, 6, 7]. Istnieje oczywiście grupa specyficznych poleceń, związanych z rolą tych urządzeń. Poniżej przedstawione są polecenia umożliwiające stworzenie konfiguracji zbliżonej do zaprezentowanej w sekcji 5.2.3 [27].

1. Tryb użytkownika uprzywilejowanego i tryb konfiguracji globalnej uruchamia się poleceniami identycznymi jak w przypadku routerów i przełączników:

```
ap>enable
ap#configure terminal
ap(config)#
```

2. Nazwę można skonfigurować poleceniem:

```
hostname nazwa
```

3. Do zabezpieczenia urządzenia hasłami służą polecenia:

```
enable secret hasło
username nazwa_użytkownika password hasło
no username Cisco
```

Oprócz wprowadzenia własnych haseł, warto również zrezygnować ze standardowej nazwy użytkownika (*Cisco*).

4. Zdalny dostęp do urządzenia jest realizowany poprzez wirtualny interfejs BVII. Domyślna jego konfiguracja ma postać:

```
interface BVII
 ip address dhcp client-id FastEthernet0
```

W razie braku serwera DHCP lub ze względów bezpieczeństwa, adres IP może być skonfigurowany statycznie:

```
ip address adres maska
```

Interfejs FastEthernet0 jest domyślnie włączony, co w razie potrzeby można zweryfikować poleceniem:

```
show ip interface brief
```

5. Kolejne polecenia służą do stworzenia SSID i ustawienia jego podstawowych parametrów:

```
dot11 ssid SSID
    authentication open
    guest-mode
```

SSID jest ciągiem złożonym z maksymalnie 32 znaków, przy czym różniane są wielkie i małe litery. **authentication open** włącza otwarte uwierzytelnianie. **guest-mode** włącza rozgłaszanie informacji o SSID (tzw. tryb gościnny) i jednocześnie dopuszcza połączenia od hostów nieposiadających skonfigurowanego SSID sieci. W przypadku skonfigurowania kilku SSID, tryb gościnny może być włączony tylko dla jednego. Pozostałe SSID będą ukryte, więc warunkiem połączenia z nimi będzie uprzednie wpisanie odpowiedniej nazwy w ustawieniach karty sieciowej hosta.

6. Interfejs radiowy należy włączyć i przypisać do niego uprzednio stworzony SSID.

```
interface dot11Radio0
    no shutdown
    ssid SSID
```

SSID stworzony na punkcie dostępowym pozostaje nieaktywny do chwili przypisania go do interfejsu radiowego. W trybie konfiguracji interfejsu można także ustawić numer kanału, poleceniem:

```
channel numer | częstotliwość | least-congested
```

Jako parametr podaje się numer kanału, centralną częstotliwość lub słowo **least-congested**. W ostatnim przypadku punkt dostępowy automatycznie wybierze najmniej wykorzystywany kanał.

7. Bieżącą konfigurację można zapisać poleceniem:

```
copy running-config startup-config
```

Informację o klientach połączonych z punktem dostępowym wyświetla polecenie:

```
show dot11 associations
```

5.2.8. Zadanie – konfiguracja poprzez wiersz poleceń IOS

Skorzystaj z sieci zbudowanej w zadaniu 5.2.5. Połącz się z wierszem poleceń punktu dostępowego, poprzez port konsolowy lub Telnet. Przywróć ustawienia fabryczne. W przypadku połączenia telnetowego, w trybie użytkownika uprzywilejowanego wprowadź polecenie:

```
terminal monitor
```

by móc śledzić komunikaty systemowe (np. informacje o przyłączeniu klienta do punktu dostępowego). Skonfiguruj punkt dostępowy, zgodnie z instrukcją podaną w powyższej sekcji 5.2.7. Komputer PC2 powinien uzyskać możliwość łączenia się z pozostałymi urządzeniami w sieci lokalnej i w Internecie, identycznie jak w zadaniu 5.2.5. Po wykonaniu zadania punkt dostępowy należy wyłączyć, ponieważ funkcjonuje on jako publicznie dostępny hotspot.

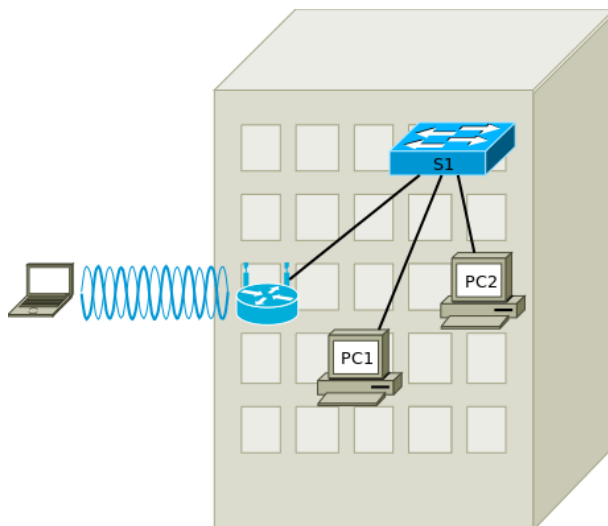
ROZDZIAŁ 6

BEZPIECZEŃSTWO SIECI BEZPRZEWODOWYCH

6.1.	Wstęp	56
6.2.	Najprostsze zabezpieczenia	57
6.3.	Zabezpieczenia kryptograficzne	58
6.3.1.	Standardy zabezpieczeń	58
6.3.2.	Konfiguracja WEP	59
6.3.3.	Zadanie – łamanie klucza WEP	60
6.3.4.	Konfiguracja osobistego WPA2	63
6.3.5.	Zadanie – osobiste WPA2	66
6.3.6.	Konfiguracja korporacyjnego WPA2	67
6.3.7.	Zadanie – konfiguracja korporacyjnego WPA2	72
6.4.	Monitorowanie sieci bezprzewodowej	72
6.5.	Podsumowanie	73

6.1. Wstęp

W sieciach bezprzewodowych ma zastosowanie większość ogólnych zaleceń odnośnie bezpieczeństwa sieci komputerowych [28]. Mają one jednak również swoją specyfikę, wymagającą implementacji dodatkowych zabezpieczeń. W sieciach przewodowych wiele mechanizmów bezpieczeństwa można zaimplementować już w warstwie fizycznej, np. prowadząc okablowanie w miejscach trudno dostępnych dla niepowołanych osób, wyłączając nieużywane porty, zamykając szafy i pomieszczenia ze sprzętem. Ze względu na rodzaj medium wykorzystywanego w sieciach bezprzewodowych, które jest dostępne dla wszystkich znajdujących się w pobliżu, tego typu sposoby zawodzą. Technicznie możliwe jest ograniczenie zasięgu sieci bezprzewodowej tylko do pomieszczeń, w których jest wykorzystywana, poprzez ekranowanie, przy użyciu farb i folii przewodzących. Takie rozwiązania są jednak kosztowne, kłopotliwe i nie gwarantują pełnej izolacji, w związku z czym ich zastosowania są niszowe. Należy więc liczyć się z ryzykiem podsłuchiwania transmisji, nielegalnego korzystania z zasobów sieci, jak również celowego lub przypadkowego zakłócenia działania.



Rysunek 6.1. Router bezprzewodowy zainstalowany przez użytkowników sieci

W związku z popularnością technologii, mechanizmy bezpieczeństwa są obecnie niezbędnym elementem każdej sieci bezprzewodowej, przy czym powinny one być adekwatne do zastosowań i wymagań stawianych danej sieci. Istotnie różni się zabezpieczanie sieci domowej i sieci korporacyjnej. W sieciach, których bezpieczeństwo ma szczególne znaczenie, z rozwiązań

bezprzewodowych rezygnuje się zupełnie. To jednak zwiększa ryzyko samowolnej instalacji urządzeń bezprzewodowych przez użytkowników (rys. 6.1). Są one poza kontrolą administratora i mogą umożliwić osobom z zewnątrz nieautoryzowany dostęp do zasobów sieci.

6.2. Najprostsze zabezpieczenia

Jednym z najprostszych sposobów poprawy bezpieczeństwa sieci bezprzewodowej jest ograniczenie jej zasięgu poprzez zmniejszenie mocy nadajnika punktu dostępowego. Może okazać się, że w średniej wielkości mieszkaniu lub niewielkim biurze, zamiast kilkudziesięciu miliwatów wystarczy kilkanaście lub nawet kilka. Można też dobrać antenę o odpowiedniej charakterystyce, by zminimalizować emisję sygnału w kierunkach, w których nie jest to potrzebne. W ten sposób jednocześnie zmniejsza się wzajemne zakłócanie sąsiednich sieci. Niektóre punkty dostępowe umożliwiają też automatyczne wyłączanie nadajnika radiowego o zadanych porach (np. poza godzinami pracy).

Większość punktów dostępowych w domyślnej konfiguracji periodycznie rozgłasza informacje o swoim SSID, umożliwiając hostom znajdującym się w ich zasięgu wykrycie sieci. W przypadku urządzeń Aironet Cisco, jest to określane mianem trybu gościnnego (ang. *guest mode*). W przypadku kilku SSID skonfigurowanych na jednym punkcie dostępowym, tryb gościnny może być włączony dla co najwyżej jednego. Hosty, które w ustawieniach karty sieciowej posiadają już wprowadzony SSID, nie potrzebują rozgłaszanych informacji. Wyłączenie rozgłaszania informacji o SSID może nieco zwiększyć bezpieczeństwo – być może pozostający w ukryciu punkt dostępowy nie wzbudzi zainteresowania potencjalnego atakującego. Sposób ten jest jednak obecnie nieskuteczny, ponieważ powszechnie dostępne oprogramowanie do analizy ruchu w sieci bezprzewodowej pozwoli uzyskać informacje o sieciach w pobliżu, jeżeli występuje jakikolwiek ruch.

Prostym sposobem uwierzytelniania urządzeń łączących się z punktem dostępowym jest sprawdzanie adresów MAC kart sieciowych (ang. *MAC address filtering*). Funkcję tę oferują prawie wszystkie punkty dostępowe. Pracować w sieci bezprzewodowej mogą tylko urządzenia, których adresy MAC znajdują się na liście. To zabezpieczenie również obecnie nie jest skuteczne. Ze względu na łatwość podsłuchiwania ruchu (sniffingu) w sieci bezprzewodowej, można łatwo uzyskać informacje o adresach MAC uprawnionych urządzeń i zmienić adres MAC karty sieciowej.

6.3. Zabezpieczenia kryptograficzne

6.3.1. Standardy zabezpieczeń

Konfigurując sieć bezprzewodową, można rozważyć implementację mechanizmów opisanych powyżej, jednak należy mieć świadomość tego, że nie gwarantują one obecnie akceptowalnego poziomu bezpieczeństwa. Dla zapewnienia poufności, integralności i uwierzytelniania, niezbędne jest zastosowanie procedur bazujących na algorytmach kryptograficznych, uznawanych aktualnie za bezpieczne.

Pierwszym takim algorytmem był WEP (ang. *Wired Equivalent Privacy*), wprowadzony w wersji 802.11 zatwierdzonej w 1999 roku. Jak wskazuje nazwa, celem jego twórców było zapewnienie poziomu bezpieczeństwa porównywalnego z sieciami przewodowymi. WEP-40 wykorzystuje 40-bitowy klucz, który połączony z 24-bitowym wektorem inicjującym, stanowi 64-bitowy klucz dla algorytmu szyfrującego RC4. Następnie wprowadzono wariant WEP-104, z 104-bitowym kluczem i 24-bitowym wektorem inicjującym. Przy konfigurowaniu urządzenia, 40-bitowy klucz można wprowadzić jako 10-cyfrową liczbę w zapisie szesnastkowym lub 5-znakowy ciąg ASCII. Klucz 104-bitowy to 26 cyfr w zapisie szesnastkowym lub 13 znaków ASCII.

WEP zakłada dwa warianty uwierzytelniania klientów: system otwarty lub uwierzytelnianie ze współdzielonym kluczem. W pierwszym przypadku, uwierzytelniony zostanie każdy host, który podejmie taką próbę. Jednak dalsza komunikacja z punktem dostępowym będzie możliwa wyłącznie pod warunkiem posiadania tego samego klucza przez obie strony. Zatem włączenie procedury uwierzytelniania na podstawie klucza nie podnosi poziomu bezpieczeństwa systemu. Co więcej, może ona ułatwić atakującemu poznanie klucza. Jednak już w 2001 roku odkryto znacznie poważniejsze wady szyfrowania WEP, umożliwiające złamanie klucza. W kolejnych latach odkrywano nowe słabości protokołu WEP, skracające czas potrzebny do przeprowadzenia ataku. Wkrótce powszechnie dostępne stały się łatwe w użyciu narzędzia (np. Aircrack-ng¹), pozwalające na zrealizowanie skutecznego ataku w ciągu zaledwie kilku minut, nawet bez znajomości szczegółów funkcjonowania protokołu. Tymczasowym rozwiązaniem problemu braku bezpieczeństwa może być zastosowanie szyfrowanych tuneli (np. IPsec).

Kolejnym mechanizmem bezpieczeństwa był WPA (*Wi-Fi Protected Access*), zdefiniowany we wstępnej wersji standardu 802.11i, wkrótce w finalnej wersji zastąpiony przez WPA2 [29]. W roku 2007, standard 802.11i został włączony do 802.11.

WPA wykorzystuje protokół TKIP (*Temporal Key Integrity Protocol*), który zapewnia szyfrowanie każdego pakietu nowym kluczem. Wyeliminowano

¹ <http://www.aircrack-ng.org/>

wano wiele słabości protokołu WEP, jednak szyfrowanie nadal odbywa się przy pomocy algorytmu RC4, którego stosowanie jest już nierekomendowane. Zdecydowano się na to, by ułatwić szybką aktualizację oprogramowania urządzeń korzystających wcześniej z WEP. Pomimo wad, WPA jest znacznie bezpieczniejsze niż WEP.

W WPA2 wykorzystuje się szyfrowanie CCMP (*Counter Cipher Mode with Block Chaining Message Authentication Code Protocol*), oparte na powszechnie stosowanym standardzie AES (*Advanced Encryption Standard*), następcy standardu DES (*Data Encryption Standard*). To rozwiązanie jest obecnie zalecane.

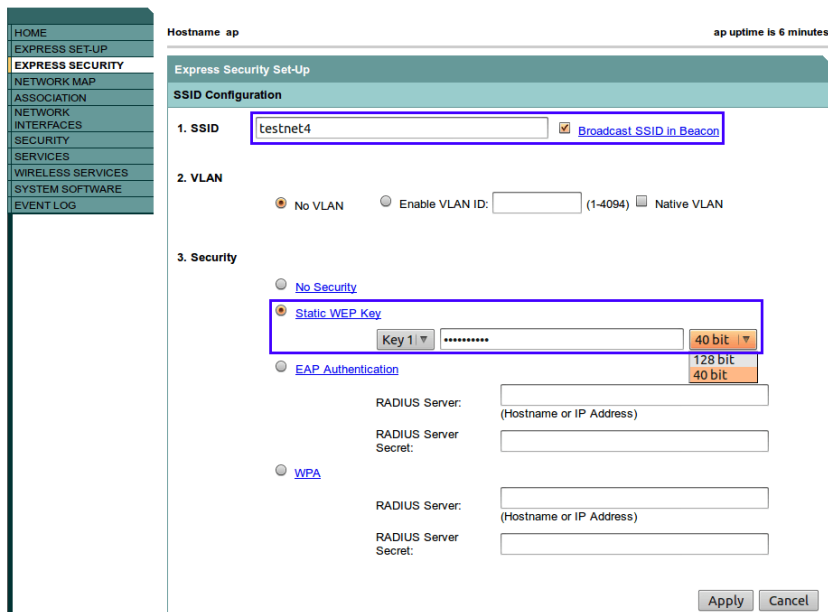
Zarówno WPA, jak i WPA2 może działać w trybie osobistym (ang. *personal*) lub korporacyjnym (ang. *enterprise*). W trybie osobistym, ze współdzielonym kluczem (WPA-PSK lub WPA2-PSK, *pre-shared key*), na wszystkich urządzeniach w sieci należy skonfigurować ten sam klucz, liczący od 8 do 63 znaków ASCII. Taki sposób zarządzania kluczem jest odpowiedni dla niewielkich sieci, z zaufanymi użytkownikami. Szczególnie istotne jest stworzenie możliwie długiego i skomplikowanego klucza, w przeciwnym razie sieć może być podatna na atak (podobnie jak w przypadku WEP, dostępne są odpowiednie narzędzia i zbiory typowych haseł).

Korporacyjne WPA (WPA2) stosuje implementację standardu IEEE 802.1x [30], dotyczącego uwierzytelniania urządzeń dołączanych do sieci lokalnej (bezprowodowej lub przewodowej), z wykorzystaniem protokołu EAP (*Extensible Authentication Protocol*), w wielu różnych wariantach (np. LEAP, EAP-TLS, EAP-MD5, EAP-FAST, PEAP, ...). Jest wówczas potrzebny serwer przechowujący bazę danych o klientach. Najczęściej używany jest do tego celu serwer RADIUS (*Remote Authentication Dial In User Service*). Istnieją liczne jego implementacje, komercyjne i otwarte. Podczas uwierzytelniania, punkt dostępowy wysyła do serwera dane urządzenia klienckiego (np. identyfikator lub adres MAC i hasło), otrzymując w odpowiedzi informację o jego akceptacji lub odrzuceniu.

6.3.2. Konfiguracja WEP

Jak już wspomniano, standard WEP nie zapewnia obecnie akceptowalnego poziomu bezpieczeństwa i nie powinien być stosowany. Opis jego konfiguracji jest związany z kolejnym zadaniem, mającym na celu wykazanie słabości tego protokołu.

W sekcji *Express Security* należy wprowadzić SSID oraz 40 lub 128-bitowy klucz WEP (rys. 6.2). Musi on zostać wprowadzony w zapisie szesnastkowym. Pozostałe ustawienia dotyczące uwierzytelniania i szyfrowania zostaną skonfigurowane automatycznie, w domyślny sposób. Pozostaje je-

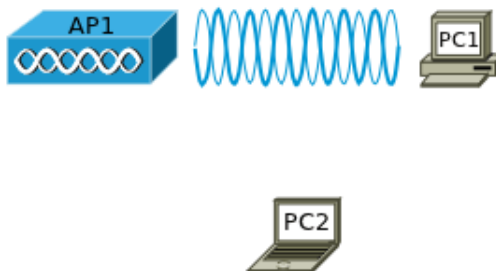


Rysunek 6.2. Podstawowa konfiguracja WEP

dynie włączenie interfejsu radiowego. Ten sam klucz należy wprowadzić na urządzeniach klienckich.

6.3.3. Zadanie – łamanie klucza WEP

Przedstawiona tu procedura ataku na protokół WEP jest powszechnie znana. Należy jednak zwrócić uwagę na fakt, że użycie jej w sieci innej niż własna, laboratoryjna, jest niezgodne z prawem.



Rysunek 6.3. Schemat topologii logicznej sieci

1. Skonfiguruj punkt dostępowy AP1 (rys. 6.3), uruchamiając na nim SSID z szyfrowaniem WEP, z 40-bitowym kluczem. Skonfiguruj komputer PC1

- tak, aby mógł nawiązać połączenie z punktem dostępowym. PC2 zostanie użyty do złamania klucza.
2. Pobierz i zainstaluj na komputerze PC2 program Aircrack-ng wraz z dodatkowymi narzędziami (<http://www.aircrack-ng.org/>), w sposób odpowiedni dla posiadanego systemu operacyjnego (Linux, Windows, Mac OSX, OpenBSD). W dalszej części zadania zakładamy, że jest to Linux. Do działania Aircrack-ng niezbędna jest jedna z obsługiwanych przez niego bezprzewodowych kart sieciowych. Szczegółowe informacje można znaleźć na stronie projektu.
 3. Należy zidentyfikować nazwę radiowego interfejsu sieciowego komputera PC2, np. poleceniem `iwconfig`:

```
$ iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wlan0      IEEE 802.11abgn  ESSID: off/any
[...]
```

W tym przykładzie jest to *wlan0*.

4. Kartę sieciową należy przełączyć w tryb monitorowania, w którym będzie odbierać wszystkie ramki, a nie tylko te, które są do niej adresowane. Tryb ten włączamy poleceniem:

```
airmon-ng start wlan0 kanał
```

podając numer kanału, na którym działa punkt dostępowy. Nazwa interfejsu (tutaj *wlan0*) musi być zgodna z funkcjonującą w systemie. Jeżeli włączenie monitorowania powiedzie się, powinien zostać wyświetlony komunikat zbliżony do poniższego:

```
Interface   Chipset   Driver

wlan0       Unknown   brcm80211 - [phy0]
              (monitor mode enabled on mon0)
```

5. Włączamy przechwytywanie ruchu, np.:

```
airodump-ng -c kanał --bssid adresMAC -w output wlan0
```

Jako parametr `-bssid` należy podać adres MAC interfejsu radiowego punktu dostępowego. Odebrane ramki będą zapisywane do pliku o nazwie *output-numer.cap*. Informacje o działaniu programu przechwytyującego ramki są na bieżąco wyświetlane na ekranie (rys. 6.4), aż do

```

CH 9 ][ Elapsed: 52 s ][ 2012-05-23 11:31
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:1D:70:9C:FA:00 -48 100 523 16087 0 9 54e.WEP WEP testnet4
BSSID          STATION          PWR Rate Lost Packets Probes
00:1D:70:9C:FA:00 00:13:E8:64:16:27 0 0 - 1 0 13
00:1D:70:9C:FA:00 78:E4:00:3F:24:E9 -54 54e-54e 0 16240

```

Rysunek 6.4. Ekran programu przechytującego ramki (airodump-ng)

chwili gdy zostanie przerwany (ctrl+c). W kolumnie #Data podawana jest informacja o liczbie przechwyconych pakietów. W przypadku 40-bitowego klucza WEP, należy zgromadzić ich co najmniej kilka tysięcy. Potrzeba na to niewiele czasu, jeżeli w sieci odbywa się intensywny ruch. W warunkach laboratoryjnych, można wysłać dużą liczbę pakietów *echo request/echo reply* między PC1 i punktem dostępowym, poleceniem *ping* z odpowiednimi parametrami. W razie prawdziwego ataku, jeżeli sieć jest mało aktywna, atakujący może wygenerować dodatkowy ruch, stosując fałszywe uwierzytelnianie lub uprzednio podsłuchany źródłowy adres MAC klienta już połączony z punktem dostępowym. Możliwe jest wprowadzanie do sieci pakietów ARP. W przypadku omawianego pakietu oprogramowania, służy do tego celu narzędzie *aireplay-ng*.

```

Opening output-07.cap
Read 57959 packets.

# BSSID          ESSID          Encryption
1 00:1D:70:9C:FA:00 testnet4      WEP (28469 IVs)

Choosing first network as target.

Opening output-07.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 28469 ivs.

Aircrack-ng 1.1

[00:00:00] Tested 92 keys (got 28469 IVs)

KB depth byte(vote)
0 0/ 3 71(40192) FA(38400) AB(37632) 72(35840) 2B(35584) CE(35328) 6C(34816) 21(34048) 03(33536)
1 0/ 2 CA(39680) E8(36352) A7(35328) 4D(34560) 95(34304) 1E(33792) 69(33792) A5(33536) C4(33536)
2 0/ 3 65(38144) 14(36096) D2(35328) 68(34560) 72(34560) F2(34048) 5E(33792) BE(33792) 37(33536)
3 0/ 2 72(38656) 19(35840) DB(35072) 34(34816) DD(34560) 6B(34304) 07(34048) 30(34048) AC(33792)
4 0/ 5 74(37888) A1(36096) B5(35584) 4D(35328) 18(34816) 44(34560) 39(34304) E7(34048) 57(33536)

KEY FOUND! [ 71:77:65:72:74 ] (ASCII: qwert )
Decrypted correctly: 100%

```

Rysunek 6.5. Wynik działania programu *aircrack-ng*

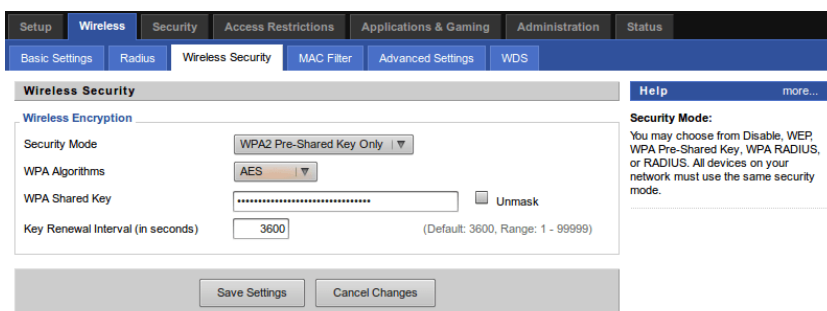
- Po zgromadzeniu odpowiedniej liczby pakietów, uruchamiamy program służący do złamania klucza:

```
aircrack-ng output-numer.cap
```

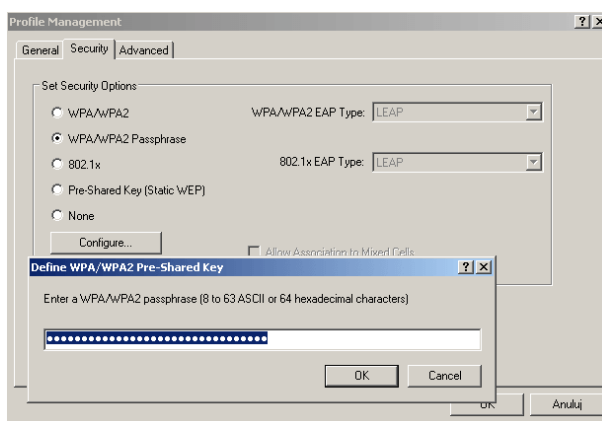
podając nazwę pliku z przechwyconymi danymi jako parametr. Nie trzeba przy tym przerywać działania programu przechwytyjącego ramki (airdump-ng). Jeżeli operacja powiedzie się, wynik działania programu będzie zbliżony do przedstawionego na rys. 6.5 – uzyskamy informację o kluczu.

W razie niepowodzenia działań zgodnych z opisaną procedurą, informacje o typowych problemach, które mogą się pojawić, jak również sposobach ich rozwiązania, można znaleźć w dokumentacji [31]. Często można spotkać karty sieciowe, których sterowniki nie w pełni współpracują z Aircrack-ng. Źródłem problemów mogą być również inne programy, które odwołują się do karty sieciowej – należy je zatrzymać.

6.3.4. Konfiguracja osobistego WPA2



Rysunek 6.6. Konfiguracja WPA2 na domowym punkcie dostępowym

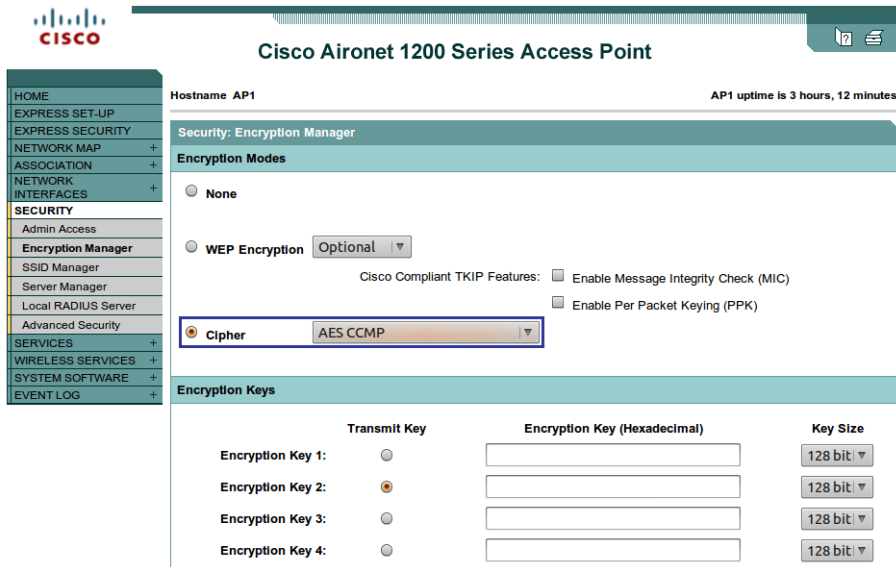


Rysunek 6.7. Konfiguracja WPA2 w ustawieniach karty sieciowej komputera

Konfiguracja WPA2 w wariantcie osobistym (*WPA2 Personal*), na punktach dostępowych przeznaczonych dla użytkowników indywidualnych i małych biur, zwykle sprowadza się do wybrania odpowiedniej opcji z menu (rys. 6.6) i wprowadzenia klucza, który następnie będzie wpisany w ustawieniach kart sieciowych urządzeń klienckich (rys. 6.7).

W przypadku urządzeń profesjonalnych, procedura jest bardziej skomplikowana i wymaga pewnej wiedzy o wykorzystywanych protokołach. Przykładowa instrukcja przedstawiona poniżej odnosi się do urządzeń serii Aironet z systemem IOS w wersji 12.3 lub nowszej. Pokazany jest sposób konfiguracji przy użyciu interfejsu graficznego. Informacje o sposobie konfiguracji poprzez wiersz poleceń można znaleźć w dokumentacji [32] lub analizując plik konfiguracyjny wygenerowany przez narzędzie graficzne. Zakładamy, że punkt dostępowy został już wstępnie skonfigurowany, z otwartym uwierzytelnianiem, w sposób opisany w sekcji 5.2.3 lub 5.2.7.

1. Należy połączyć się z punktem dostępowym przy pomocy przeglądarki WWW i z menu po lewej stronie wybrać *Security – Encryption Manager*. Następnie ustawiamy szyfrowanie (*Cipher*) odpowiednie dla WPA2, czyli AES CCMP – rys. 6.8. Wybór, jak w każdym przypadku, trzeba zatwierdzić przyciskiem *Apply* w dolnej części strony.



Rysunek 6.8. WPA2 – ustawienie szyfrowania

2. Wybieramy *Security – SSID Manager*. Można stworzyć nowy SSID do wykorzystania z WPA2 (opcja *NEW* na liście SSID) lub wybrać jeden

z istniejących (*net4free* w przykładzie z rys. 6.9). Następnie zaznaczamy otwarte uwierzytelnianie (*Open Authentication*) – rys. 6.9.

The screenshot shows the configuration interface for a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point" and the hostname is "AP1". The status bar indicates "AP1 uptime is 1 hour, 28 minutes".

The left sidebar contains a navigation menu with the following items: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY (highlighted), Admin Access, Encryption Manager, SSID Manager (highlighted), Server Manager, Local RADIUS Server, Advanced Security, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG.

The main content area is titled "Security: Global SSID Manager" and "SSID Properties". It shows the "Current SSID List" with a table containing one entry: "net4free". To the right of the list are fields for "SSID:" (set to "net4free"), "VLAN:" (set to "< NONE >"), "Backup 1:", "Backup 2:", "Backup 3:", "Interface:" (set to "Radio0-802.11G"), and "Network ID:" (set to "(0-4096)"). A "Delete" button is located below the list.

The "Client Authentication Settings" section shows "Methods Accepted:" with three options: "Open Authentication:" (checked), "Shared Authentication:" (unchecked), and "Network EAP:" (unchecked). Each option has a dropdown menu set to "< NO ADDITION >".

Rysunek 6.9. WPA2 – uwierzytelnianie

3. W dalszej części tej samej strony konfigurujemy klucz dla WPA2 (który następnie zostanie wpisany w ustawieniach WPA2 kart sieciowych wszystkich urządzeń w sieci) i sposób zarządzania nim: *Key Management: Mandatory, WPA*, a poniżej wpisujemy klucz – rys. 6.10. Ustawienia należy zatwierdzić przyciskiem *Apply*, znajdującym się w tej samej sekcji, co modyfikowane parametry (na stronie są dwie sekcje, z dwoma niezależnymi przyciskami *Apply*).

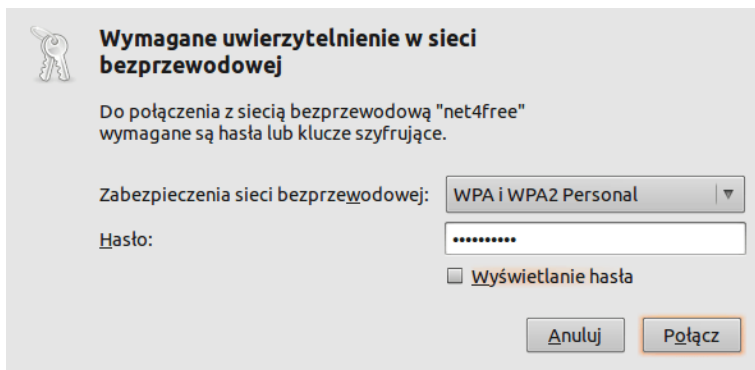
The screenshot shows the "Client Authenticated Key Management" configuration page. It features two main sections:

The first section is "Key Management:" with a dropdown menu set to "Mandatory". To its right are two checkboxes: "CCKM" (unchecked) and "WPA" (checked).

The second section is "WPA Pre-shared Key:" with a text input field containing a series of dots. To its right are two radio buttons: "ASCII" (selected) and "Hexadecimal" (unselected).

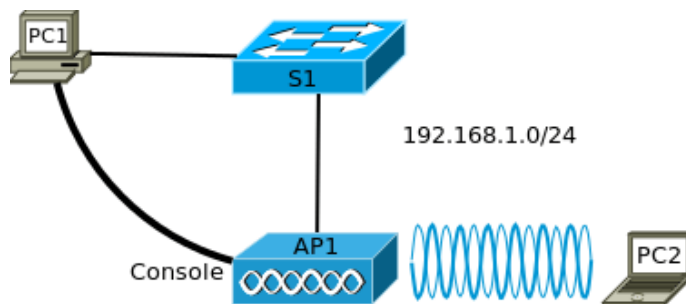
Rysunek 6.10. WPA2 – konfiguracja klucza

- Po włączeniu WPA2, w ustawieniach kart sieciowych hostów i wpisaniu klucza, zgodnego z wprowadzonym przy konfiguracji WPA2 na punkcie dostępowym, powinno udać się nawiązanie bezpiecznego, szyfrowanego połączenia z punktem dostępowym (rys. 6.11).



Rysunek 6.11. WPA2 – przykładowa konfiguracja hosta

6.3.5. Zadanie – osobiste WPA2



Rysunek 6.12. Schemat topologii logicznej sieci

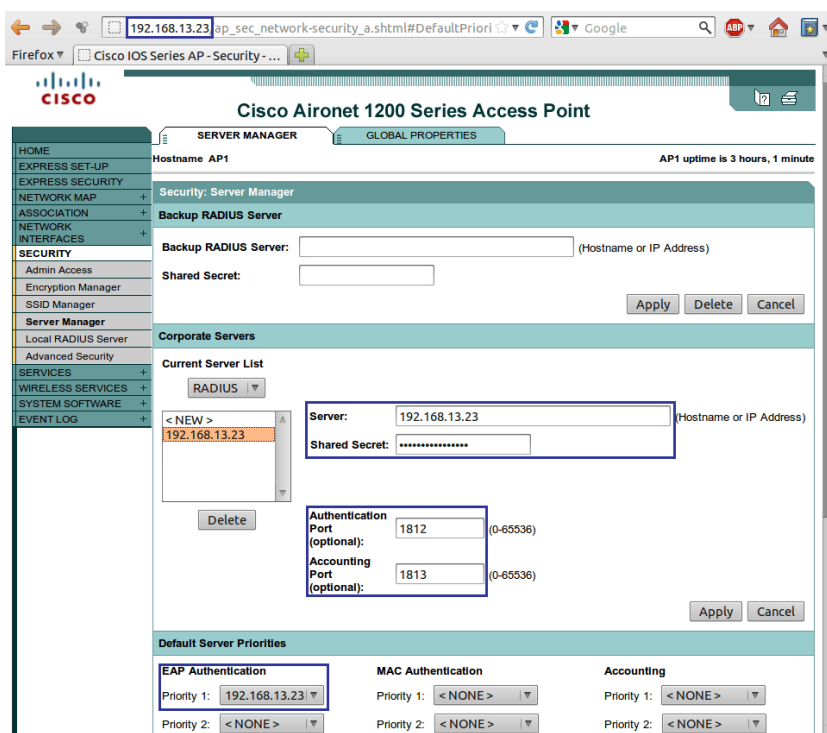
- Zbuduj sieć zgodnie ze schematem (rys. 6.12). Nawiąż połączenie konsolowe z punktem dostępowym. Przypisz interfejsowi BVI1 punktu dostępowego statyczny adres IP z sieci 192.168.1.0/24 i skonfiguruj na nim serwer DHCP dla sieci lokalnej. Upewnij się, że komputer PC1 otrzymuje poprawny adres od serwera DHCP.
- Skonfiguruj na punkcie dostępowym SSID z otwartym uwierzytelnianiem i uruchom interfejs radiowy. Upewnij się, że komputer PC2 łączy się z siecią bezprzewodową i może komunikować się z PC1 (ping).

3. Korzystając z powyższej instrukcji (sekcja 6.3.4), zaimplementuj na punkcie dostępowym AP1 WPA2 w wariantcie osobistym, z dowolnie wybranym kluczem. Sprawdź, że komputer PC2 stracił możliwość połączenia z siecią. Skonfiguruj w ustawieniach jego bezprzewodowej karty sieciowej WPA2 z kluczem identycznym jak na punkcie dostępowym. Ponownie zweryfikuj możliwość komunikacji w sieci.

6.3.6. Konfiguracja korporacyjnego WPA2

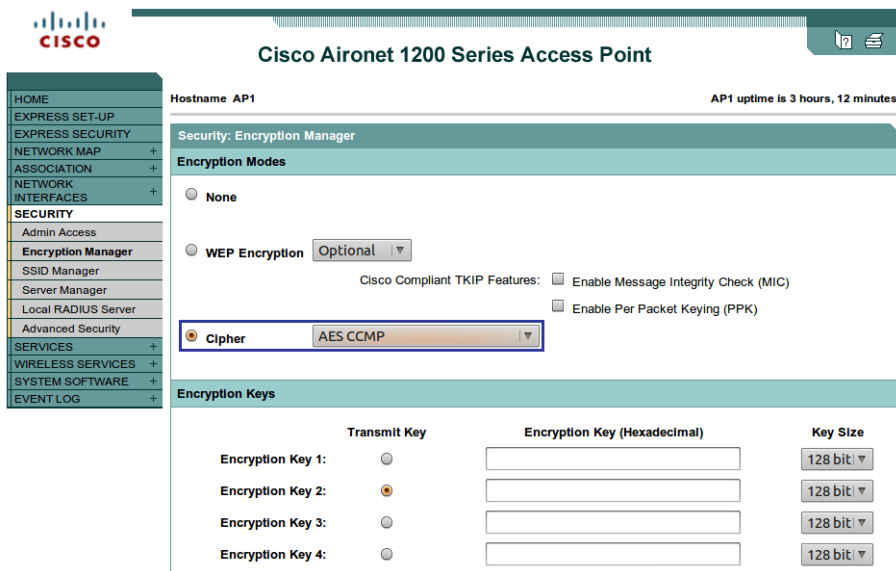
Przedstawiony zostanie przykład konfiguracji WPA2 z uwierzytelnianiem zgodnym z protokołem LEAP (*Cisco Lightweight Extensible Authentication Protocol*). Użyty będzie serwer Radius uruchomiony bezpośrednio na punkcie dostępowym (IOS oferuje taką usługę, jednak jego możliwości są ograniczone). W przypadku rozbudowanych sieci z dużą liczbą użytkowników, zalecane jest dysponowanie dedykowanym serwerem do uwierzytelniania.

Zakładamy, że podstawowa konfiguracja punktu dostępowego została już przeprowadzona i możemy połączyć się z nim poprzez przeglądarkę WWW.



Rysunek 6.13. Konfiguracja serwera Radius

1. Zaczynamy od wprowadzenia parametrów serwera Radius, który ma być wykorzystywany, w sekcji *Security – Server Manager*. Ustalamy adres serwera Radius na identyczny z adresem punktu dostępowego, ponieważ serwer zostanie uruchomiony na konfigurowanym urządzeniu. Serwer Radius będzie korzystał z portów 1812 i 1813 i będzie domyślnym serwerem uwierzytelniania EAP – rys. 6.13. *Shared Secret* jest hasłem zabezpieczającym połączenie z serwerem Radius, które musi być znane urządzeniom korzystającym z serwera.



Rysunek 6.14. WPA2 – ustawienie szyfrowania

2. W sekcji *Security – Encryption Manager* wybieramy szyfrowanie AES CCMP – rys. 6.14.
3. W sekcji *Security – SSID Manager* wybieramy SSID lub tworzymy nowy (w naszym przykładzie *abcCorp*) – rys. 6.15. W przypadku urządzeń klienckich firmy Cisco, należy skonfigurować uwierzytelnianie *Network EAP*, natomiast dla urządzeń innych firm – *Open Authentication with EAP*. Można wybrać również oba warianty.
4. W dalszej części tej samej strony konfigurowujemy sposób zarządzania kluczem: *Key Management: Mandatory, WPA* – rys. 6.16. Ustawienia zatwierdzamy przyciskiem *Apply*.
5. Skonfigurowania wymaga jeszcze lokalny serwer Radius. W sekcji *Security – Local Radius Server*, w zakładce *General Set-Up*, wybieramy *LEAP* i zatwierdzamy – rys. 6.17. Na tej samej stronie wprowadzamy adres IP i hasło serwera Radius, identyczne jak w 1. kroku instrukcji. Ustawie-

The screenshot shows the configuration interface for a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point" and the hostname is "AP1". The uptime is "3 hours, 22 minutes". The left sidebar contains navigation options: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY (highlighted), Admin Access, Encryption Manager, SSID Manager (highlighted), Server Manager, Local RADIUS Server, Advanced Security, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled "Security: Global SSID Manager" and "SSID Properties". It features a "Current SSID List" with entries: "< NEW >", "abcCorp", and "net4free". A "Delete" button is below the list. To the right, the "SSID:" field is set to "abcCorp", "VLAN:" is set to "< NONE >", and "Interface:" is set to "Radio0-802.11G". The "Network ID:" field is empty. Below this is the "Client Authentication Settings" section, where "Methods Accepted:" includes "Open Authentication:" set to "with EAP", "Shared Authentication:" set to "< NO ADDITION >", and "Network EAP:" set to "< NO ADDITION >".

Rysunek 6.15. WPA2 – uwierzytelnianie

The screenshot shows the "Client Authenticated Key Management" configuration page. The "Key Management:" dropdown is set to "Mandatory". There are checkboxes for "CCKM" (unchecked) and "WPA" (checked). Below this is the "WPA Pre-shared Key:" field, which is empty. To the right of the field are radio buttons for "ASCII" (selected) and "Hexadecimal" (unselected).

Rysunek 6.16. WPA2 – zarządzanie kluczem

nia zatwierdzamy przyciskiem *Apply*. W dalszej części tego samego okna wprowadzamy identyfikatory i hasła poszczególnych użytkowników – rys. 6.18.

6. Protokół uwierzytelniania i dane użytkowników muszą zostać skonfigurowane na poszczególnych hostach. Przykładową konfigurację w systemie Linux Ubuntu przedstawia rys. 6.19. Niektóre narzędzia dostarczone przez producentów kart sieciowych szczegółowo informują o przebiegu procesu uwierzytelniania – rys. 6.20.

Cisco Aironet 1200 Series Access Point

STATISTICS GENERAL SET-UP EAP-FAST SET-UP

Hostname AP1 AP1 uptime is 3 hours, 51 minutes

Security: Local RADIUS Server - General Set-Up

Local Radius Server Authentication Settings

Enable Authentication Protocols:

- EAP FAST
- LEAP
- MAC

Apply Cancel

Network Access Servers (AAA Clients)

Current Network Access Servers

< NEW >
192.168.13.23

Network Access Server: 192.168.13.23 (IP Address)

Shared Secret:

Delete

Apply Cancel

Individual Users

Rysunek 6.17. Podstawowa konfiguracja serwera Radius

Individual Users

Current Users

< NEW >
karol

Delete

Username: karol

Password:

Confirm Password:

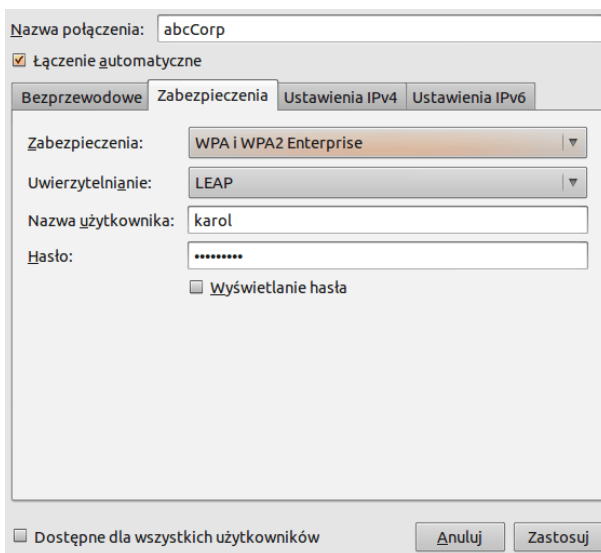
Group Name: < NONE >

Text NT Hash

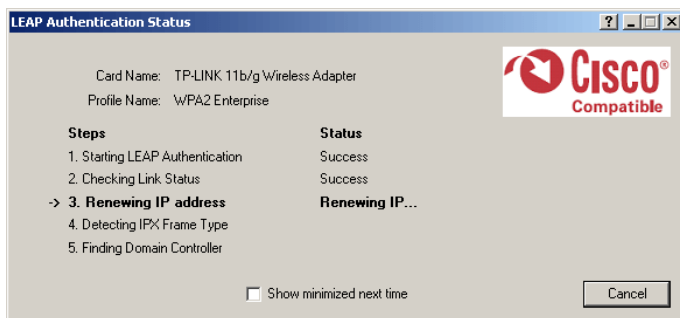
MAC Authentication Only

Apply Cancel

Rysunek 6.18. Zakładanie kont użytkowników na serwerze Radius



Rysunek 6.19. Konfiguracja klienta – Linux Ubuntu



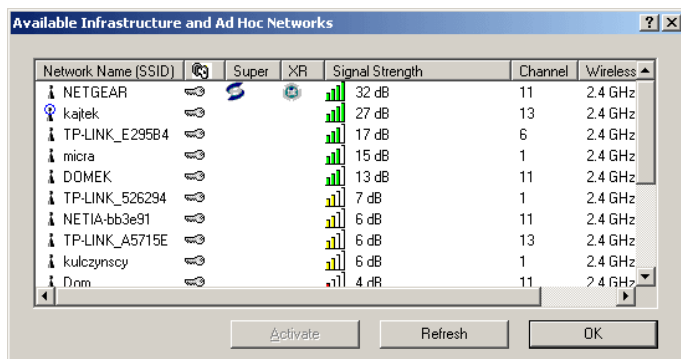
Rysunek 6.20. Przebieg uwierzytelniania WPA2

6.3.7. Zadanie – konfiguracja korporacyjnego WPA2

Skorzystaj z sieci zbudowanej w zadaniu 6.3.5 (rys. 6.12). Na punkcie dostępowym uruchom i skonfiguruj serwer Radius, do uwierzytelniania klientów łączących się z siecią bezprzewodową. Załóż jedno lub więcej kont dla użytkowników. Do istniejącej konfiguracji z poprzedniego zadania dodaj kolejny SSID, z korporacyjnym WPA2. Skonfiguruj komputer PC2 tak, by połączył się z nowo utworzonym SSID, uwierzytelniając się przy pomocy wybranego identyfikatora i hasła.

6.4. Monitorowanie sieci bezprzewodowej

Ze względu na naturę sieci bezprzewodowych, szczególne znaczenie ma stałe monitorowanie sytuacji. Znajdują tu zastosowanie narzędzia wykorzystywane w sieciach przewodowych (np. analizatory logów, protokół SNMP i RMON, sniffery), lecz nie są one wystarczające.



Rysunek 6.21. Wybór kanału radiowego

Jednym z pierwszych problemów, na które natrafia się już na etapie uruchamiania sieci, jest wybór jak najmniej zakłócanego kanału radiowego. Może w tym pomóc np. narzędzie dołączone do karty sieciowej (rys. 6.21) lub linuksowe polecenie

```
iwlist [interface] scanning
```

Są jednak również znacznie bardziej rozbudowane programy, również dla urządzeń przenośnych z systemem Android.

Jednym z najbardziej znanych programów do wykrywania lokalnych sieci bezprzewodowych, podsłuchiwania ruchu i wykrywania pewnych zdarzeń

Network List (Packets desc)							Info
Name	T	W	Ch	Packts	Flags	IP Range	Size
! TP-LINK_BC83723	A	0	006	1470		0.0.0.0	9k
! Agnieszka	A	0	003	1346		0.0.0.0	0B
! TP-LINK_E295B4	A	0	006	1289		0.0.0.0	273B
! Home_Nett	A	0	006	1228		0.0.0.0	0B
! qumak_sekom	A	0	004	902		0.0.0.0	0B
! NETGEAR	A	0	011	774		0.0.0.0	0B
! NETIA-bb3e91	A	0	011	757		0.0.0.0	0B
! micra	A	0	001	670		0.0.0.0	0B
! DOMEK	A	0	011	516		0.0.0.0	2k
! TP-LINK_526294	A	0	001	418		0.0.0.0	0B
! Iffonna	A	N	006	418	U4	94.72.113.212	6k
! kulczynscy	A	0	001	388		0.0.0.0	1k
! Lubisz	A	Y	011	376		0.0.0.0	0B
. kdom	A	0	011	363		0.0.0.0	0B
! pandora	A	0	006	341		0.0.0.0	0B
! dlink	A	0	006	340		0.0.0.0	360B
! Dom	A	Y	011	339		0.0.0.0	3k
! SAMSUNG	A	0	002	296		0.0.0.0	0B
! linksys	A	0	001	267		0.0.0.0	0B
. Ana	A	0	001	162		0.0.0.0	0B
! kajtek	A	0	013	153		0.0.0.0	360B
. Natalia_WiFi_6149	A	0	002	142		0.0.0.0	0B
TP-LINK_B7305c	A	0	004	125		0.0.0.0	0B
domek2	A	Y	011	63		0.0.0.0	0B
dlink	A	N	010	17		0.0.0.0	0B

88% (+) Down

Status
 ALERT: Suspicious client 78:E4:00:16:FB:51 - probing networks but never participating.
 Sorting by packet counts (descending)
 ALERT: Suspicious client 7A:79:05:74:B7:9A - probing networks but never participating.
 ALERT: Suspicious client 00:E0:4C:B4:0E:BA - probing networks but never participating.
Battery: AC charging 90%

Info
 Ntwrks: 28
 Pckets: 14584
 Cryptd: 115
 Weak: 0
 Noise: 1
 Discrd: 1
 Pkts/s: 34
 addme
 Ch: 36
 Elapsed: 00:09:31

Rysunek 6.22. Główne okno programu Kismet

jest Kismet² – rys. 6.22. Kismet działa wyłącznie pasywnie, tzn. zbiera wszystkie ramki, które uda się odebrać, przeskakując między różnymi kanałami radiowymi. W ten sposób można zdobyć informacje o punktach dostępowych (również ukrytych) i połączonych z nimi klientach. Przechwycone ramki można następnie analizować, np. przy użyciu programu Wireshark³. Kismet wykrywa również niektóre podejrzane zachowania w sieci (np. próby skanowania aktywnego, po których nie następuje asocjacja z siecią) i na bieżąco o nich informuje.

Kismet może ułatwić wykrycie nieautoryzowanych urządzeń bezprzewodowych zainstalowanych w sieci. Zaawansowane punkty dostępowe mają natomiast tego typu funkcje zaimplementowane fabrycznie. Na podstawie informacji z kilku sąsiednich punktów dostępowych, można dość dokładnie określić lokalizację poszukiwanego urządzenia.

6.5. Podsumowanie

Obecnie przyjmuje się, że standard WPA2, przy wykorzystaniu odpowiednio skomplikowanych haseł, zapewnia rozsądny poziom bezpieczeństwa sieci bezprzewodowej. Nie gwarantuje go natomiast WEP, ukrywanie SSID

² <http://www.kismetwireless.net/>

³ <http://www.wireshark.org/>

ani filtrowanie adresów MAC. Trzeba jednak mieć świadomość faktu, że zagrożenia są tu bardzo zróżnicowane. Istnieje wiele tzw. niestandardowych metod ataku, w przypadku których nie istnieją proste środki zaradcze.

Źródłem zagrożeń bywają także działania użytkowników, którzy mogą do sieci firmy dołączać własne urządzenia bezprzewodowe, lub nieświadomie łączyć się z punktem dostępowym zainstalowanym w celu przechwytywania ruchu sieciowego (w tym danych o tożsamości).

Zapewnianie bezpieczeństwa nie jest zatem jednorazową czynnością, lecz procesem, który powinien być stale prowadzony, w sposób adekwatny do zagrożeń i wymagań stawianych danej sieci.

ROZDZIAŁ 7

BEZPRZEWODOWE WIRTUALNE SIECI LOKALNE

7.1. Wstęp	76
7.2. Konfiguracja VLAN na punktach dostępowych Aironet	76
7.3. Zadanie	81
7.4. Wskazówki do zadania 7.3	82

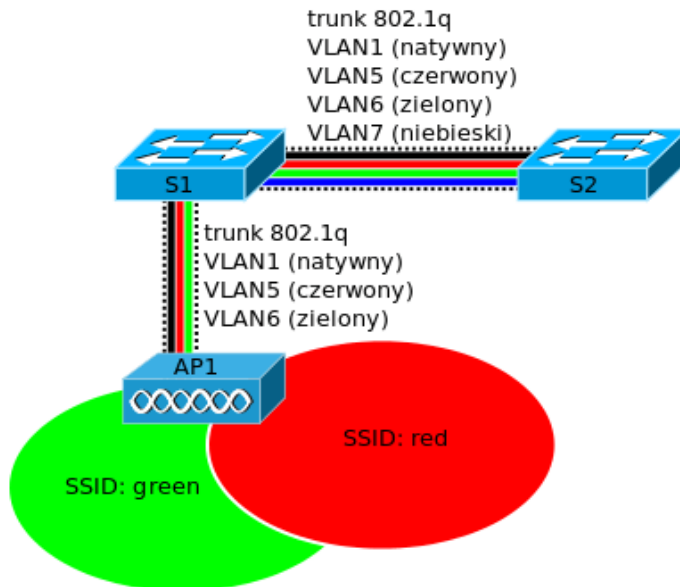
7.1. Wstęp

W sieciach lokalnych Ethernet często tworzy się wirtualne sieci LAN (VLAN). Logiczne wydaje się więc rozszerzenie technologii VLAN również na sieci bezprzewodowe. Więcej informacji na ten temat konfigurowania sieci VLAN na przełącznikach Cisco Catalyst można znaleźć w [6].

Urządzenia Aironet serii 1200 umożliwiają skonfigurowanie maksymalnie 16 SSID, które mogą być jednocześnie aktywne i każdy z nich może mieć różne ustawienia bezpieczeństwa. Można powiązać SSID z określoną siecią VLAN, przy czym jednej sieci VLAN można przypisać tylko jeden SSID. Hosty połączone z danym SSID automatycznie należą do powiązanej z nim sieci VLAN i mogą wysyłać i odbierać ramki tylko w jej obrębie.

7.2. Konfiguracja VLAN na punktach dostępowych Aironet

W przykładowej sieci z rys. 7.1, skonfigurowano 3 sieci VLAN (z identyfikatorami 5, 6 i 7). Postanowiono jednak, że bezprzewodowo będą dostępne tylko VLAN5 i VLAN6. Punkt dostępowy jest połączony z przełącznikiem Ethernet poprzez łącze *trunk* (802.1q). Na punkcie dostępowym uruchomiono dwa SSID: *Red* i *Green*, które zostały skojarzone z VLAN5 i VLAN6, odpowiednio.



Rysunek 7.1. Bezprzewodowe sieci VLAN

Aby uniknąć różnego rodzaju problemów, budując tego typu sieci, powinno się przestrzegać następujących zaleceń:

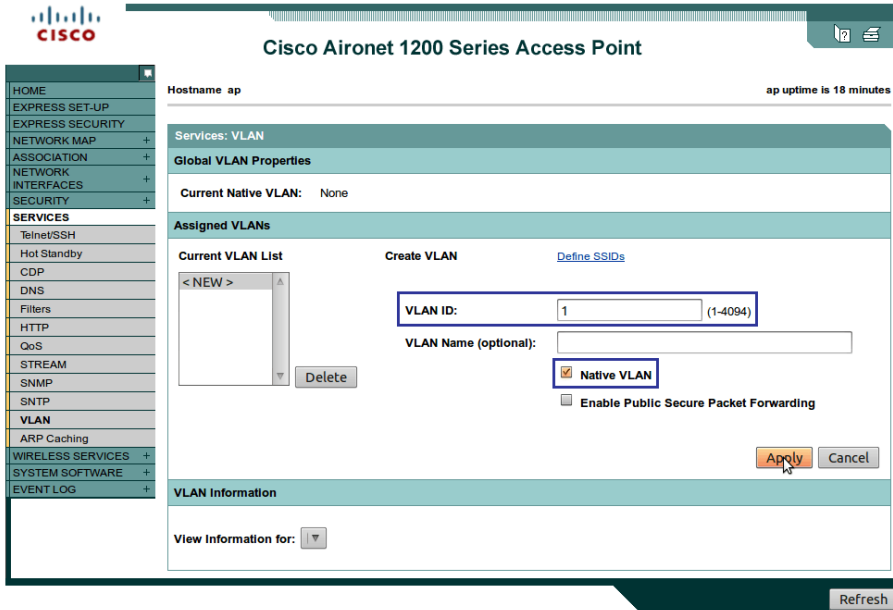
- Zestawiając połączenie *trunk* między przełącznikiem a punktem dostępowym, po stronie przełącznika należy skonfigurować dokładnie te sieci VLAN, które są zdefiniowane na punkcie dostępowym (w przykładzie z rysunku, VLAN 5 i 6 ma być udostępniony bezprzewodowo, VLAN1 będzie używany do zarządzania punktem dostępowym, natomiast zrezygnowano z VLAN7).
- Należy zwrócić uwagę, by natywny VLAN (ang. *native VLAN*, w polskojęzycznej literaturze nazywany także rodzimym) był identycznie skonfigurowany po obu stronach łącza *trunk*. Interfejs zarządzający punktu dostępowego (BV11, wykorzystywany również do uwierzytelniania klientów) zawsze należy do natywnej sieci VLAN (przy czym nie musi to być VLAN1), co trzeba wziąć pod uwagę przy planowaniu adresowania IP.
- Ze względów bezpieczeństwa, do natywnej sieć VLAN nie powinien być przypisywany SSID.
- Urządzenia Aironet nie obsługują protokołu DTP (*Dynamic Trunking Protocol*), więc należy połączenie *trunk* skonfigurować statycznie. Zalecane jest wyłączenie negocjowania po stronie przełącznika (polecenie `switchport nonegotiate`).

Poniższe punkty przedstawiają krok po kroku sposób konfiguracji punktu dostępowego i przełącznika S1 (Catalyst) w sieci z rys. 7.1, w celu udostępnienia sieci VLAN 5 i 6 bezprzewodowo [33]. Zakładamy, że punkt dostępowy posiada adres IP i możemy połączyć się z nim przeglądarką WWW, a sieci VLAN na przełącznikach są już skonfigurowane.

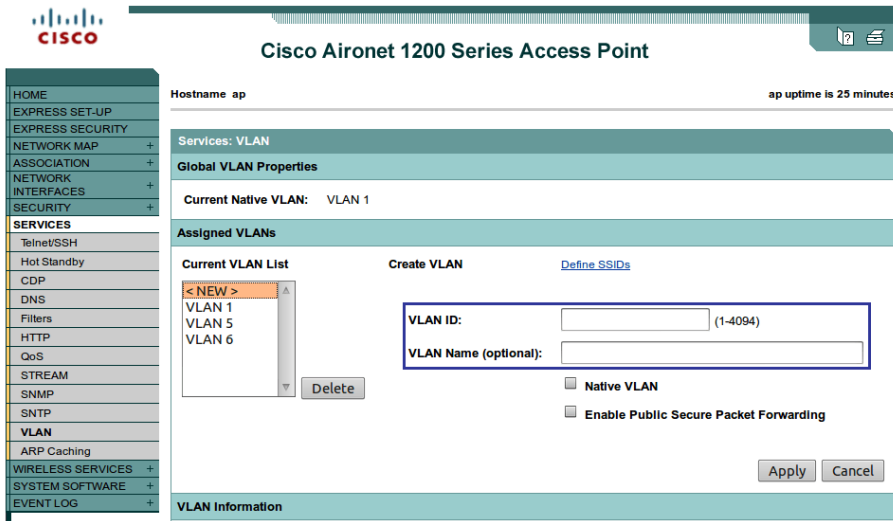
1. Na przełączniku konfigurujemy połączenie *trunk* z punktem dostępowym:

```
interface FastEthernet0/1
  switchport mode trunk
  switchport trunk encapsulation dot1q
  switchport nonegotiate
  switchport trunk allowed vlan 1,5,6
  switchport trunk native vlan 1
```

2. Po połączeniu się przeglądarką WWW z punktem dostępowym, wybieramy *Services – VLAN* – rys. 7.2. Klikamy *New*, w miejscu wskazanym na rysunku wpisujemy identyfikator natywnej sieci VLAN (w naszym przypadku 1), zaznaczamy “Native VLAN” i zatwierdzamy przyciskiem *Apply*.
3. Analogicznie tworzymy VLAN 5 i 6, przy czym nie zaznaczamy już opcji “Native VLAN”. Można również sieciom VLAN nadać nazwy – rys. 7.3.
4. Skonfigurowane już sieci VLAN należy powiązać z SSID. Wybieramy

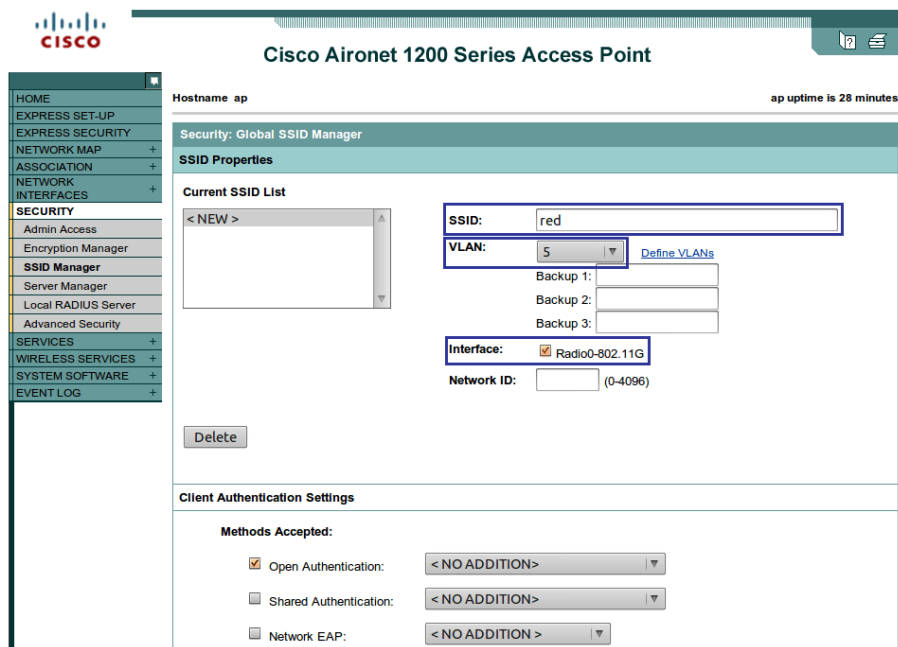


Rysunek 7.2. Konfiguracja natywnej sieci VLAN na punkcie dostępowym



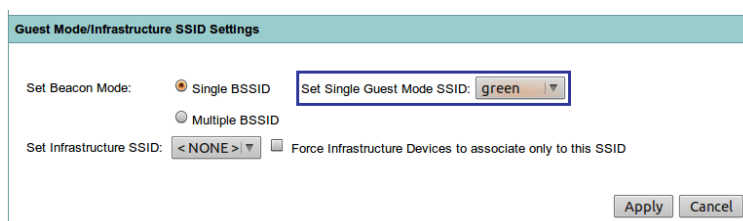
Rysunek 7.3. Konfiguracja sieci VLAN na punkcie dostępowym

Security – SSID Manager. W miejscu wskazanym na rys. 7.4 wpisujemy nowy SSID, wybieramy numer sieci VLAN, z którym ma być powiązany i zaznaczamy interfejs radiowy. Ustawienia zatwierdzamy przyciskiem



Rysunek 7.4. Konfiguracja powiązania sieci VLAN i SSID

Apply. Analogicznie tworzymy drugi SSID (*green*, skojarzony z VLAN6). Sieci natywnej (w naszym przykładzie VLAN1) nie przypisujemy do żadnego SSID, ze względów bezpieczeństwa.



Rysunek 7.5. Włączanie rozgłaszania wybranego SSID

W dolnej części tego samego ekranu konfiguracyjnego można włączyć rozgłaszanie informacji o jednym, wybranym SSID (pozostałe będą ukryte) – rys. 7.5.

- Ostatnią czynnością konfiguracyjną jest włączenie (domyślnie wyłączono) interfejsu radiowego, w sposób przedstawiony w Rozdziale 5.
- Poprawność powiązania sieci VLAN z SSID oraz mechanizmy bezpieczeństwa poszczególnych SSID można sprawdzić w miejscu pokazanym

na rys. 7.6. Sieć *green* powinna zostać automatycznie wykryta przez komputery znajdujące się w zasięgu punktu dostępowego, natomiast *red* pozostanie ukryta (konieczne będzie ręczne wpisanie SSID w ustawieniach połączenia sieciowego).

Cisco Aironet 1200 Series Access Point

Hostname **ap** ap uptime is 38 minutes

Security Summary

Administrators

Username	Read-Only	Read-Write
Cisco		

Service Set Identifiers (SSIDs)

SSID	VLAN	Radio	BSSID/Guest Mode	Open	Shared	Network EAP
green	6	Radio0-802.11G	001d.709c.fa00	no addition		
red	5	Radio0-802.11G	001d.709c.fa00	no addition		

Encryption Settings

VLAN	Encryption Mode	WEP		Cipher						Key Rotation
		MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	AES CCM	
1	None									
5	None									
6	None									

Rysunek 7.6. Weryfikacja powiązania sieci VLAN z SSID

Kolejny listing zawiera polecenia umożliwiające skonfigurowanie powiązań sieci VLAN i SSID poprzez wiersz poleceń.

Listing 7.1. Konfiguracja sieci VLAN i powiązania ich z SSID

```

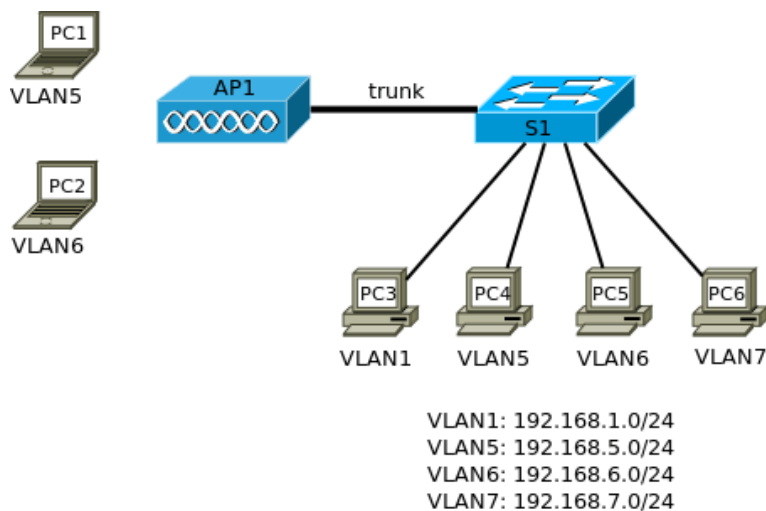
1 dot11 vlan-name czerwony vlan 5
2 dot11 vlan-name zielony vlan 6
3 !
4 dot11 ssid green
5     vlan 6
6     authentication open
7     guest-mode
8 !
9 dot11 ssid red
10    vlan 5
11    authentication open
12 !
13 interface Dot11Radio0
14 !
15     ssid green
16 !
17     ssid red
18 !
19 !

```



```
20 interface Dot11Radio0.1
   encapsulation dot1Q 1 native
22 !
   interface Dot11Radio0.5
24   encapsulation dot1Q 5
   !
26 interface Dot11Radio0.6
   encapsulation dot1Q 6
28 !
   interface FastEthernet0.1
30   encapsulation dot1Q 1 native
   !
32 interface FastEthernet0.5
   encapsulation dot1Q 5
34 !
   interface FastEthernet0.6
36   encapsulation dot1Q 6
   !
```

7.3. Zadanie



Rysunek 7.7. Schemat topologii logicznej sieci

1. Połącz urządzenia zgodnie ze schematem z rys. 7.7. Do przeprowadzenia doświadczeń, wystarczy jeden komputer w sieci przewodowej i jeden w bezprzewodowej.

2. Stwórz na przełączniku VLAN 5, 6 i 7. W każdej z sieci (również VLAN1) skonfiguruj interfejs wirtualny (`interface vlan`) i przypisz mu najniższy możliwy adres IP.
3. Na przełączniku skonfiguruj serwer DHCP (wskazówki można znaleźć w Dodatku A.1), definiując pule adresów dla każdej z sieci.
4. Przypisz wybrane porty przełącznika do dowolnych, spośród uprzednio stworzonych sieci VLAN. Dołączone do nich komputery powinny otrzymać odpowiednie adresy od serwera DHCP. Komputer, który będzie wykorzystywany do konfigurowania punktu dostępowego, pozostaw w VLAN1.
5. Skonfiguruj (po stronie przełącznika) połączenie *trunk* tak, aby obsługiwało VLAN 1 (natywne), 5 i 6.
6. Punkt dostępowy powinien otrzymać od serwera DHCP adres IP z sieci VLAN1 (informację o przydzielonych adresach można uzyskać na przełączniku poleceniem `show ip dhcp binding`). Połącz się z nim telnetem (aby konfigurować poprzez wiersz poleceń) lub przeglądarką WWW (aby konfigurować przy użyciu interfejsu graficznego).
7. Na punkcie dostępowym skonfiguruj VLAN 1 (natywne), 5, 6. VLAN5 skojarz z SSID *red*, natomiast VLAN6 z SSID *green*. Włącz rozgłaszanie informacji o SSID *green*.
8. Korzystając z komputera z bezprzewodową kartą sieciową, upewnij się, że sieć *green* jest wykrywana. Połącz się z nią i sprawdź, czy host otrzymał adres z odpowiedniej puli (192.168.6.0/24). Sprawdź, czy można łączyć się (ping) z interfejsem VLAN6 przełącznika lub dowolnym hostem należącym do VLAN6.
9. Połącz się z ukrytą siecią *red*. Komputer powinien otrzymać adres z sieci 192.168.5.0/24 i mieć możliwość komunikacji z interfejsem VLAN5 przełącznika i innymi hostami należącymi do VLAN5.

7.4. Wskazówki do zadania 7.3

Wskazówki odnośnie sposobu skonfigurowania punktu dostępowego można znaleźć w sekcji 7.2. Poniższy listing przedstawia istotne elementy konfiguracji przełącznika S1.

Listing 7.2. Istotne elementy konfiguracji przełącznika S1

```
1 ip dhcp pool PULA1
   network 192.168.1.0 255.255.255.0
3 !
   ip dhcp pool PULA5
5   network 192.168.5.0 255.255.255.0
   !
```

```
7 ip dhcp pool PULA6
   network 192.168.6.0 255.255.255.0
9 !
ip dhcp pool PULA7
11  network 192.168.7.0 255.255.255.0
   !
13 interface FastEthernet0/1
   switchport trunk allowed vlan 1,5,6
15  switchport mode trunk
   !
17 interface FastEthernet0/2
   !
19 interface FastEthernet0/3
   !
21 interface FastEthernet0/4
   !
23 interface FastEthernet0/5
   switchport access vlan 5
25  switchport mode access
   !
27 interface FastEthernet0/6
   switchport access vlan 6
29  switchport mode access
   !
31 interface FastEthernet0/7
   switchport access vlan 7
33  switchport mode access
   !
35 interface Vlan1
   ip address 192.168.1.1 255.255.255.0
37  no shutdown
   !
39 interface Vlan5
   ip address 192.168.5.1 255.255.255.0
41  no shutdown
   !
43 interface Vlan6
   ip address 192.168.6.1 255.255.255.0
45  no shutdown
   !
```

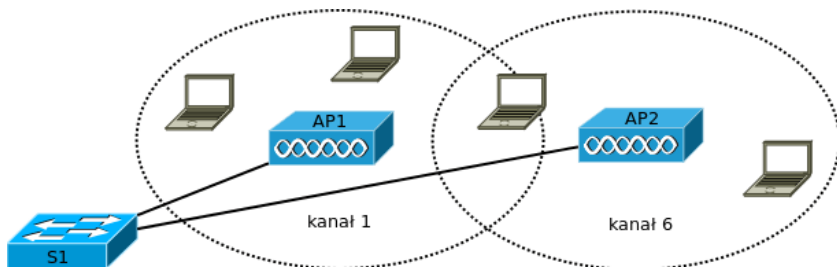
ROZDZIAŁ 8

PRZEKAŹNIKI I MOSTY BEZPRZEWODOWE

8.1.	Wstęp	86
8.2.	Mosty bezprzewodowe w otwartej przestrzeni	88
8.3.	Konfiguracja punktu dostępowego Aironet w roli przekaźnika bezprzewodowego	90
8.4.	Zadanie – przekaźnik bezprzewodowy	92
8.5.	Konfiguracja mostu bezprzewodowego z urządzeniami Aironet	92
8.6.	Zadanie – konfiguracja mostu bezprzewodowego	96
8.7.	Zadanie – konfiguracja mostu grupy roboczej	96

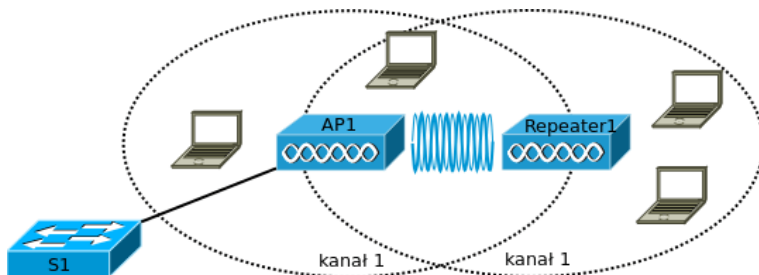
8.1. Wstęp

Rys. 8.1 przedstawia typowy, rekomendowany sposób rozbudowy lokalnej sieci bezprzewodowej, w sytuacji gdy jeden punkt dostępowy (AP1) nie jest w stanie zapewnić połączenia z siecią w całym obszarze, w którym jest to potrzebne. Instalowany jest kolejny punkt dostępowy (AP2), skonfigurowany z tym samym SSID, wykorzystujący inny, odpowiednio odległy kanał radiowy.



Rysunek 8.1. Rozbudowa sieci bezprzewodowej o kolejne punkty dostępowe

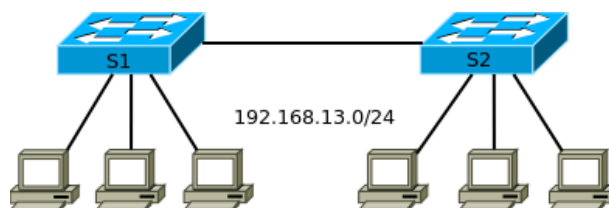
W pewnych sytuacjach, wykonanie przewodowego połączenia między punktem dostępowym a przełącznikiem Ethernet może być trudne do wykonania. Można wówczas skorzystać z przełącznika bezprzewodowego (ang. *wireless repeater*) – rys. 8.2. Działanie przełącznika polega na retransmisji odbieranych ramek należących do danego SSID, w tym samym kanale, w którym działa punkt dostępowy. Przełącznik nie ma połączenia przewodowego i musi znajdować się w zasięgu punktu dostępowego. Urządzenia w sieci mogą dokonać asocjacji z punktem dostępowym bezpośrednio lub poprzez przełącznik.



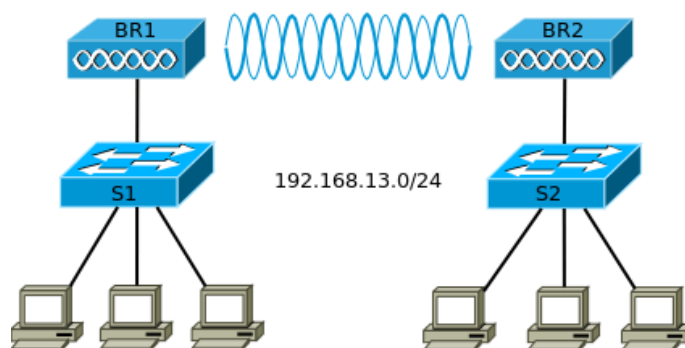
Rysunek 8.2. Rozbudowa sieci bezprzewodowej, z wykorzystaniem przełącznika

Ponieważ przełącznik i punkt dostępowy pracują na tym samym kanale radiowym, włączenie przełącznika skutkuje zmniejszeniem wydajności sieci

o około 50%. Można stworzyć łańcuch złożony z kilku przełączników, jednak na jego końcu wydajność sieci będzie bardzo niewielka. Dlatego z przełączników korzysta się tylko w ostateczności, gdy dostępu do sieci nie da się zapewnić w inny sposób, a jej szybkość nie jest priorytetem.



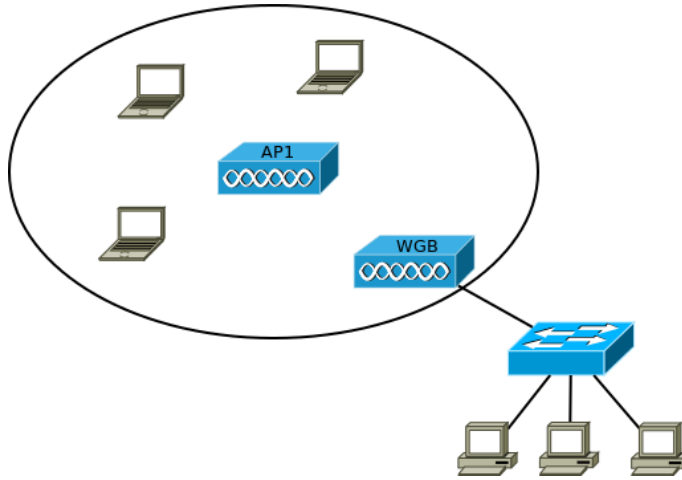
Rysunek 8.3. Sieć Ethernet z dwoma przełącznikami



Rysunek 8.4. Sieć z mostami bezprzewodowymi

Rys. 8.3 przedstawia prostą sieć Ethernet, w której zastosowano dwa przełączniki. Przewodowe połączenie między nimi można zastąpić łączem radiowym, przy wykorzystaniu mostów bezprzewodowych (ang. *wireless bridge*) – rys. 8.4. Pod względem logicznym, obie sieci zachowują się identycznie. Komputery nadal pozostają w tej samej domenie rozgłoszeniowej i ich konfiguracja IP nie wymaga zmian. Niektóre mosty bezprzewodowe mogą, jednocześnie z zapewnianiem połączenia między dwiema lokalizacjami, pełnić rolę punktów dostępowych dla znajdujących się w pobliżu hostów.

W sieci z rys. 8.5 zastosowano most grupy roboczej (ang. *workgroup bridge*). Punkt dostępowy AP1 umożliwia połączenie z siecią bezprzewodową urządzeniom znajdującym się w jego zasięgu. Most grupy roboczej (WGB) pozwala dołączyć do niej również urządzenia nieposiadające bezprzewodowych kart sieciowych.



Rysunek 8.5. Zastosowanie mostu grupy roboczej (WGB)

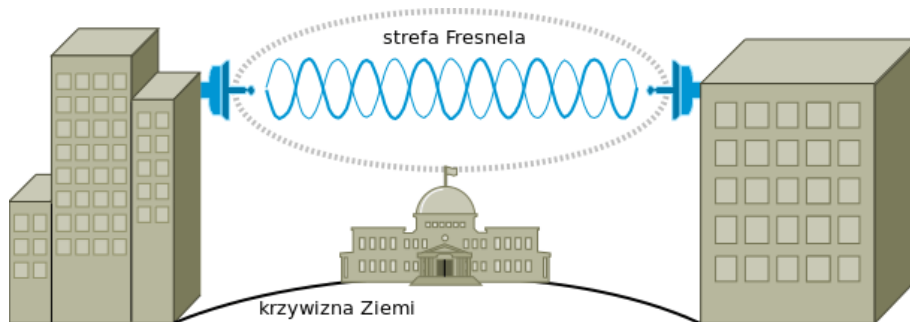
8.2. Mosty bezprzewodowe w otwartej przestrzeni

Przy użyciu anten kierunkowych, stosując mosty bezprzewodowe można zestawić połączenie o znacznej długości. Jest ono wartą rozważenia alternatywą dla rozwiązań WAN, chociaż w Europie możliwości są tu bardziej ograniczone niż np. w Stanach Zjednoczonych, ze względu na obowiązujące normy EIRP (Rozdział 2).



Rysunek 8.6. Punkt dostępowy/most bezprzewodowy, przeznaczony do instalacji na zewnątrz (Aironet serii 1300 [34])

Funkcję mostów bezprzewodowych mogą pełnić punkty dostępowe, wyposażone w taką opcję. Dedykowane mosty bezprzewodowe różnią się od nich przede wszystkim posiadaniem obudowy i złącz odpornych na niekorzystne warunki zewnętrzne (rys. 8.6). Takie urządzenie można umieścić w bezpośrednim sąsiedztwie anteny, minimalizując straty sygnału w kablu antenowym.



Rysunek 8.7. Połączenie radiowe między odległymi punktami

Cisco Systems		For Cisco Aironet 2.4GHz Outdoor Links ONLY!	
Regulatory Domain	United States/Canada		
Site 1		Site 2	
Select Device	APR-BR1310G w/remote antenna	Select Device	APR-BR1310G w/integrated antenna
Select Data Rate	54		
Modulation Type	OFDM		
Select Antenna 1 Here	21dBiOh	Select Antenna 2 Here	Integrated 13dB Patch
For other Antenna-Enter Gain Here	0.00	For other Antenna-Enter Gain Here	0.00
Power levels permitted are based on antenna gain, modulation mode (based on data rate) and regulatory domain			
Select Power level	10mW	Select Power level	30mW
Select Cable 1	20ft standard cable	Select Cable 2	NO Cable
For 'OTHER' Cable		For 'OTHER' Cable	
Enter Cable Loss dB/100 ft here	0.00	Enter Cable Loss dB/100 ft here	0.00
Enter in Length Here	0	Enter in Length Here	0
Note: When using integrated antennas, cable is not used in calculations			
Effective Isotropic Radiated Power (dBm)	29.66	Effective Isotropic Radiated Power (dBm)	29
Environmental Conditions			
Terrain	Average terrain with some roughness		
Atmosphere	Normal, interior continent, temperate or sub-arctic		
Max Distance (w/ min 5dB Link Margin)	1.52 Miles	2.45 Kilometers	
Earth Bulge at above distance	5 Feet	1.5 Meters	
Fresnel Zone clearance for above distance	17 Feet	5.2 Meters	
Required antenna height above obstructions	22 Feet	6.7 Meters	
Recommended Fade Margin (factor of distance)	5 dB		

Rysunek 8.8. Kalkulator połączeń mostowych [35]

Warunkiem koniecznym, ale nie wystarczającym, zrealizowania połączenia radiowego między odległymi miejscami jest wzajemna widoczność komunikujących się anten (rys. 8.7). Dodatkowo, w przestrzeni powinien być wol-

ny od przeszkód obszar strefy Fresnela, przypominający kształtem elipsoidę obrotową. Ze względu na wykorzystywaną długość fali, istotną przeszkodą nie powinny być zjawiska atmosferyczne, w przeciwieństwie do budynków lub drzew. Trzeba to uwzględnić przy planowaniu wysokości, na której zostaną umieszczone anteny. Przy odległościach rzędu kilku kilometrów, nie można zaniedbać także krzywizny Ziemi. Przeprowadzenie dokładnych obliczeń, uwzględniających wszystkie czynniki, jest trudne, jednak producenci sprzętu sieciowego zwykle dostarczają narzędzi umożliwiających oszacowanie parametrów połączenia. Rys. 8.8 przedstawia kalkulator dla urządzeń Aironet. Po wprowadzeniu szeregu parametrów (między innymi zysku anten, rodzaju kabli, mocy nadajnika), otrzymujemy informację o maksymalnej odległości i wysokości na jakiej należy umieścić anteny, uwzględniając strefę Fresnela i krzywiznę Ziemi.

8.3. Konfiguracja punktu dostępowego Aironet w roli przełącznika bezprzewodowego

Załóżmy, że w sieci z rys. 8.2 punkt dostępowy AP1 został skonfigurowany w standardowy sposób, opisany w Rozdziale 5. Stworzony został przykładowy SSID *testnet3*, z następującymi ustawieniami:

```
dot11 ssid testnet3
  authentication open
  guest-mode
```

Przypisano go do interfejsu radiowego:

```
interface Dot11Radio0
  ssid testnet3
  station-role root
```

Rola urządzenia (*station-role root*) jest ustawieniem domyślnym.

Drugi punkt dostępowy zostanie skonfigurowany jako przełącznik. Najlepiej użyć do tego celu połączenia konsolowego, ponieważ po skonfigurowaniu dla urządzenia roli przełącznika, interfejs Ethernet przestanie działać. Oba punkty dostępowe muszą mieć włączone rozszerzenia Aironet (*Aironet extensions*), co jest ustawieniem domyślnym (ich wyłączenie może w pewnych przypadkach poprawić współpracę urządzeń Cisco z urządzeniami innych producentów). W sieci z przełącznikami Cisco mogą wystąpić problemy z komunikacją z urządzeniami klienckimi wyposażonymi w interfejsy sieciowe innych firm.

Na przełączniku konfigurujemy ten sam SSID, co na głównym punkcie dostępowym, w następujący sposób:

```
dot11 ssid testnet3
    authentication open
    infrastructure-ssid
```

przy czym sposób uwierzytelniania (**authentication**) musi być zgodny ze skonfigurowanym na AP1. SSID infrastruktury (**infrastructure-ssid**) zostanie wykorzystany do asocjacji między przekaźnikiem i punktem dostępowym i musi być przypisany do natywnej sieci VLAN. W zwykły sposób przypisujemy SSID do interfejsu radiowego, odpowiednio określając rolę urządzenia:

```
interface Dot11Radio0
    station-role repeater
    ssid testnet3
```

Szybkości transmisji punktu dostępowego i przekaźnika muszą być zgodne.

Jeżeli przekaźnik znajduje się w zasięgu punktu dostępowego, powinna nastąpić asocjacja obu urządzeń, co można zweryfikować w sposób pokazany na poniższych listingach (8.1, 8.2).

Listing 8.1. Weryfikacja asocjacji na punkcie dostępowym AP1

```
1 AP1#show dot11 associations
3 802.11 Client Stations on Dot11Radio0:
5 SSID [testnet3] :
7 MAC Addr. IP address Device      Name      Parent    State
  [...]89 ff 192.168.7.4 ap1200-Rptr Repeater1 self     Assoc
9 [...]24 e9 192.168.7.3 Rptr-client -        [...]89 ff Assoc
```

Listing 8.2. Weryfikacja asocjacji na przekaźniku (Repeater1)

```
1 Repeater1#show dot11 associations
3 802.11 Client Stations on Dot11Radio0:
5 SSID [testnet3] :
7 MAC Addr. IP address Device      Name Parent State
  [...]1170 192.168.7.1 ap1200-Parent AP1 -     Assoc
9 [...]24 e9 192.168.7.3 unknown   -     self  Assoc
```

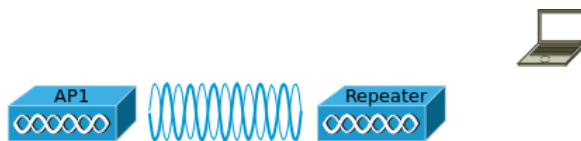
W 8. wierszu obu listingów znajduje się informacja o asocjacji między przekaźnikiem a punktem dostępowym. 9. wiersz zawiera natomiast informację

o asocjacji hosta. Jeżeli host połączy się z siecią za pośrednictwem przełącznika, informacja o nim pojawi się na obu urządzeniach (jak w powyższym przykładzie). Jeżeli natomiast bezpośrednio z punktem dostępowym, wówczas przełącznik nie będzie dysponował żadną informacją.

Standardowo przełącznik dokonuje asocjacji z punktem dostępowym o zadanym SSID, którego sygnał jest najsilniejszy. Opcjonalnie, w trybie konfiguracji interfejsu radiowego, można zdefiniować adresy MAC maksymalnie 4 punktów dostępowych, z którymi kolejno będą podejmowane próby połączenia:

```
parent {1-4} adresMAC
```

8.4. Zadanie – przełącznik bezprzewodowy



Rysunek 8.9. Schemat topologii logicznej sieci

1. Skonfiguruj punkt dostępowy AP1 z otwartym uwierzytelnianiem (rys. 8.9). Uruchom na nim serwer DHCP.
2. Skonfiguruj drugi punkt dostępowy (*Repeater*) w roli przełącznika, z tym samym SSID co AP1. Upewnij się że nastąpiła asocjacja między urządzeniami. Przełącznik powinien otrzymać adres IP od serwera DHCP.
3. Spróbuj umieścić urządzenia w taki sposób, by do komputera z bezprzewodową kartą sieciową docierał silniejszy sygnał od przełącznika niż od punktu dostępowego. Skonfiguruj komputer tak, żeby połączył się z siecią bezprzewodową. Przejrzyj informacje o asocjacji (korzystając z wiersza poleceń lub interfejsu graficznego).

8.5. Konfiguracja mostu bezprzewodowego z urządzeniami Aironet

Poniżej przedstawiony jest przykładowy sposób konfiguracji urządzeń Aironet w roli mostów bezprzewodowych, w celu budowy sieci z rys. 8.4 [37]. Jedno z urządzeń (w naszym przykładzie BR1) musi pełnić rolę mostu

głównego (ang. *root bridge*). Połączenie radiowe może nawiązać z nim jedno lub więcej urządzeń niepełniących tej roli (*non-root bridge*, w prezentowanym przykładzie – BR2).

1. Konfigurację rozpoczynamy od BR1. Łączymy się z nim przeglądarką WWW. W sekcji *Express Setup* nadajemy nazwę i konfigurujemy jako most główny – rys. 8.10. W tym miejscu lub w ustawieniach interfejsu radiowego może być dostępnych więcej opcji, np. most główny (lub most nie będący głównym) z klientami, czyli pełniący jednocześnie rolę zwykłego punktu dostępowego.

The screenshot displays the 'Express Set-Up' configuration interface. On the left is a navigation menu with options like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled 'Express Set-Up' and includes the following fields and options:

- Host Name:** BR1
- MAC Address:** 0021.55ff.399a
- Configuration Server Protocol:** DHCP (selected), Static IP
- IP Address:** 192.168.13.23
- IP Subnet Mask:** 255.255.255.0
- Default Gateway:** 0.0.0.0
- SNMP Community:** defaultCommunity
- SNMP Read/Write:** Read-Only (selected), Read-Write
- Radio0-802.11G Role in Radio Network:** Access Point, Repeater, Non-Root Bridge, Workgroup Bridge, Scanner, and Root Bridge (selected).
- Optimize Radio Network for:** Throughput, Range, Default (selected), Custom
- Aironet Extensions:** Enable (selected), Disable

Rysunek 8.10. Konfiguracja mostu głównego

2. Tworzymy nowy SSID i przypisujemy do interfejsu radiowego – rys. 8.11. W razie potrzeby można skonfigurować również mechanizmy uwierzytelniania. W dolnej części tego samego ekranu konfiguracyjnego ustawiamy SSID infrastruktury – rys. 8.12.
3. Ostatnią czynnością przy konfiguracji BR1 jest włączenie interfejsu radiowego, w zwykły sposób. Należy też zanotować jego adres MAC (czyli BSSID), ponieważ będzie potrzebny do skonfigurowania BR2.
4. Łączymy się przeglądarką WWW z BR2. Identycznie jak na BR1, tworzymy SSID i wybieramy go jako SSID infrastruktury – rys. 8.11 i 8.12.
5. W sekcji *Express Setup* nadajemy nazwę i określamy rolę urządzenia jako *non-root Bridge* (most niebędący mostem głównym) – rys. 8.14.

Hostname BR1 BR1 uptime is 15 minutes

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >
most1

SSID: most1

VLAN: < NONE > [Define VLANs](#)

Backup 1:

Backup 2:

Backup 3:

Interface: Radio0-802.11G

Network ID: (0-4096)

Delete

Client Authentication Settings

Methods Accepted:

Open Authentication: < NO ADDITION >

Shared Authentication: < NO ADDITION >

Network EAP: < NO ADDITION >

Rysunek 8.11. Konfiguracja SSID

Guest Mode/Infrastructure SSID Settings

Set Beacon Mode: Single BSSID Multiple BSSID

Set Single Guest Mode SSID: < NONE >

Set Infrastructure SSID: most1 Force Infrastructure Devices to associate only to this SSID

Apply Cancel

Rysunek 8.12. SSID infrastruktury

Home: Summary Status		
Network Identity		
IP Address	192.168.13.23	
MAC Address	0021.55ff.399a	
Network Interfaces		
Interface	MAC Address	Transmission Rate
FastEthernet	0021.55ff.399a	100Mb/s
Radio0-802.11G	0021.d833.1170	54.0Mb/s

Rysunek 8.13. Adres MAC interfejsu radiowego mostu głównego

Hostname ap ap uptime is 34 minutes

Express Set-Up

Host Name:

MAC Address: 001f.ca64.89ff

Configuration Server Protocol: DHCP Static IP

IP Address:

IP Subnet Mask:

Default Gateway:

SNMP Community:

Read-Only Read-Write

Radio0-802.11G

Role In Radio Network: Access Point Repeater Non-Root Bridge Root Bridge Workgroup Bridge Scanner

Optimize Radio Network for: Throughput Range Default Custom

Aironet Extensions: Enable Disable

Rysunek 8.14. Konfiguracja mostu niebędącego mostem głównym

Beacon Period: (20-4000 Kusec) Data Beacon Rate (DTIM): (1-100)

Max. Data Retries: (1-128) RTS Max. Retries: (1-128)

Fragmentation Threshold: (256-2346) RTS Threshold: (0-2347)

Root Parent Timeout: (0-65535 sec)

Root Parent MAC 1 (optional): (HHHH.HHHH.HHHH)

Root Parent MAC 2 (optional): (HHHH.HHHH.HHHH)

Root Parent MAC 3 (optional): (HHHH.HHHH.HHHH)

Root Parent MAC 4 (optional): (HHHH.HHHH.HHHH)

Rysunek 8.15. Konfiguracja adresu MAC mostu głównego

Hostname BR1 BR1 uptime is 48 minutes

Association

Clients: 0 Repeaters: 1

View: Client Repeater

Radio0-802.11G

SSID most1 :

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
11g-bridge	BR2	192.168.13.27	001d.709c.f900	Associated	self	none

Rysunek 8.16. Weryfikacja asocjacji urządzeń

6. W sekcji *Network Interfaces – Radio0-802.11G – Settings*, oprócz włączenia interfejsu radiowego, należy wprowadzić zanotowany uprzednio adres MAC interfejsu bezprzewodowego mostu głównego – rys. 8.15.
7. Jeżeli konfiguracja została przeprowadzona poprawnie, powinna nastąpić asocjacja obu urządzeń (rys. 8.16) i połączenie między dwoma segmentami LAN powinno zacząć funkcjonować.

8.6. Zadanie – konfiguracja mostu bezprzewodowego

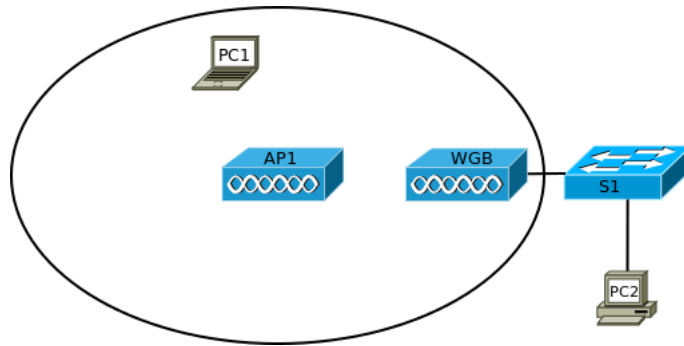


Rysunek 8.17. Schemat topologii logicznej sieci

1. Połącz urządzenia zgodnie ze schematem (rys. 8.17). Możesz pominąć przełączniki Ethernet, łącząc komputery bezpośrednio z punktami dostępowymi Aironet. Przypisz urządzeniom adresy IP z sieci 192.168.1.0/24, statycznie lub wykorzystując serwer DHCP.
2. Punkty dostępowe Aironet skonfiguruj w roli mostów bezprzewodowych. Upewnij się, że nastąpiła asocjacja między nimi.
3. Przetestuj komunikację między komputerami dołączonymi do różnych przełączników.

8.7. Zadanie – konfiguracja mostu grupy roboczej

1. Połącz urządzenia zgodnie ze schematem (rys. 8.18). Możesz pominąć przełącznik S1, łącząc komputer PC2 bezpośrednio z punktem dostępowym WGB.
2. Przeprowadź podstawową konfigurację punktu dostępowego AP1. Ustaw dowolne SSID, z otwartym uwierzytelnianiem. Upewnij się, że komputer PC1 może połączyć się z siecią bezprzewodową.



Rysunek 8.18. Schemat topologii logicznej sieci

3. Drugi punkt dostępowy Aironet (WGB) skonfiguruj w roli mostu grupy roboczej, tak aby komputery podłączone do przełącznika S1 mogły komunikować się z hostami w sieci bezprzewodowej¹.
4. Upewnij się, że nastąpiła asocjacja między AP1 i WGB oraz że komputery PC1 i PC2 mogą się ze sobą komunikować.

¹ Niniejszy podręcznik nie zawiera szczegółowych instrukcji odnośnie konfiguracji mostów grupy roboczej. Rozwiązanie zadania może wymagać skorzystania z dokumentacji, np. [36]

ROZDZIAŁ 9

INTEGROWANIE BEZPRZEWODOWYCH ROZWIĄZAŃ W SIECIACH LOKALNYCH

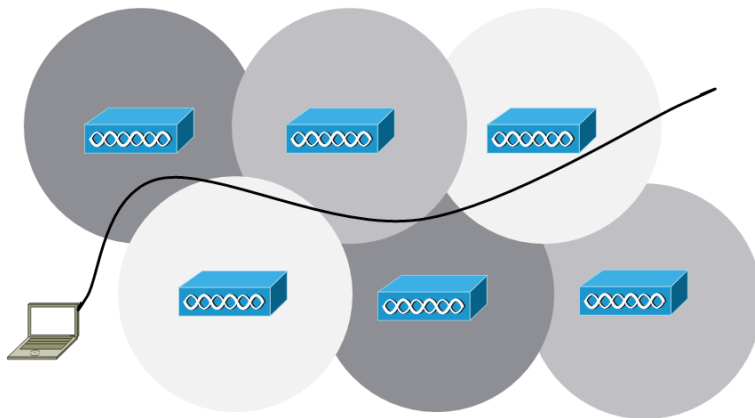
9.1. Wstęp	100
9.2. Protokoły LWAPP i CAPWAP	101
9.3. Przykładowa konfiguracja kontrolera WLAN	103
9.4. Konfiguracja kontrolera WLAN z użyciem wiersza poleczeń	107
9.5. Konfigurowanie kontrolera WLAN przez przeglądarkę WWW	109
9.6. Zadanie	115

9.1. Wstęp

Jak już wspomniano w poprzednich rozdziałach, sieci bezprzewodowe dają możliwość rozszerzania warstwy dostępu dla użytkowników końcowych bez użycia kabli dając, przy poprawnym rozmieszczeniu punktów dostępu, możliwość swobodnego połączenia do sieci. Punkty dostępu stanowią most pomiędzy danymi przesyłanymi w sposób bezprzewodowy, a zwykłą siecią lokalną (kablową), lub też tworzą pojedyncze połączenie bezprzewodowe pomiędzy odległymi punktami będącymi często w dużej odległości.

Wadą rozwiązań pojedynczych punktów dostępu jest ich ograniczony obszar działania. Dlatego też w sieciach bezprzewodowych opracowano technologie, w których można tworzyć połączenia kaskadowe dla sieci bezprzewodowych, dając tym samym możliwość funkcjonowania sieci LAN na dużym obszarze bez użycia okablowania.

Innym problemem pojawiającym się w budowaniu sieci bezprzewodowych był roaming, czyli przemieszczanie się użytkowników. Aby rozszerzyć obszar działania sieci WLAN umieszcza się punkty dostępu, w taki sposób, aby zasięg ich komórek pokrywał cały obszar, w którym może pojawić się klient. W praktyce obszary zasięgu muszą pokrywać się w pewnym niewielkim zakresie. W takim przypadku, tak jak było to już pokazane na rysunku 2.8, punkty te muszą pracować na różnych niezakłócających częstotliwościach.



Rysunek 9.1. Układ punktów dostępu zapewniający pełne pokrycie dla całego obszaru

Kiedy klient zostanie powiązany z jednym punktem zasięgu, może swobodnie się przemieszczać. Kiedy przenosi się z jednej komórki punktu dostępu do drugiej jego powiązanie powinno przejść do kolejnej. Funkcja ta nosi nazwę roamingu. Dane klienta przekazywane tuż przed roamingiem

są również przekazywane ze starego punktu do nowego. Inne rozwiązanie nie jest możliwe, ponieważ klient w jednej chwili może być połączony tylko z jednym punktem.

9.2. Protokoły LWAPP i CAPWAP

W tradycyjnej architekturze sieci bezprzewodowych komunikacja skupiona jest wokół rozproszonych punktów dostępu. Każdy punkt stanowi centralny punkt swojego własnego zbioru usług podstawowych. Jest on więc autonomiczny – w takim przypadku zarządzanie bezpieczeństwem jest zdecentralizowane. W sieci nie istnieje miejsce do monitorowania całego ruchu, ochrony przed intruzami, obsługi jakości usług (QoS), nadzorowania pasma itp. Zarządzanie częstotliwościami, mocą nadajników wielu niezależnych punktów jest kłopotliwe i dość trudne. Administrator takiej sieci odpowiada za konfigurację każdego z punktów indywidualnie. Po poprawnym skonfigurowaniu takiej sieci monitorowanie, wykrywanie wrogich punktów dostępu, działanie związane ze zmianą konfiguracji w przypadku awarii jest również bardzo trudne.

Z powodu powyższych trudności zostały zaproponowane rozwiązania scentralizowane i ujednoczone. W nowym podejściu do budowy sieci bezprzewodowych Cisco zaoferowało zastąpienie rozwiązań tradycyjnych (opartych o autonomiczne punkty dostępu) rozwiązaniami zunifikowanymi z centralnym punktem kontroli działania sieci (*Cisco Unified Wireless Network*).

W wyniku nowego podejścia, został opracowany protokół LWAPP (*Lightweight Access Point Protocol*) [8], którego założenia stały się podstawą standardu CAPWAP (*Control And Provisioning of Wireless Access Points*) [38].



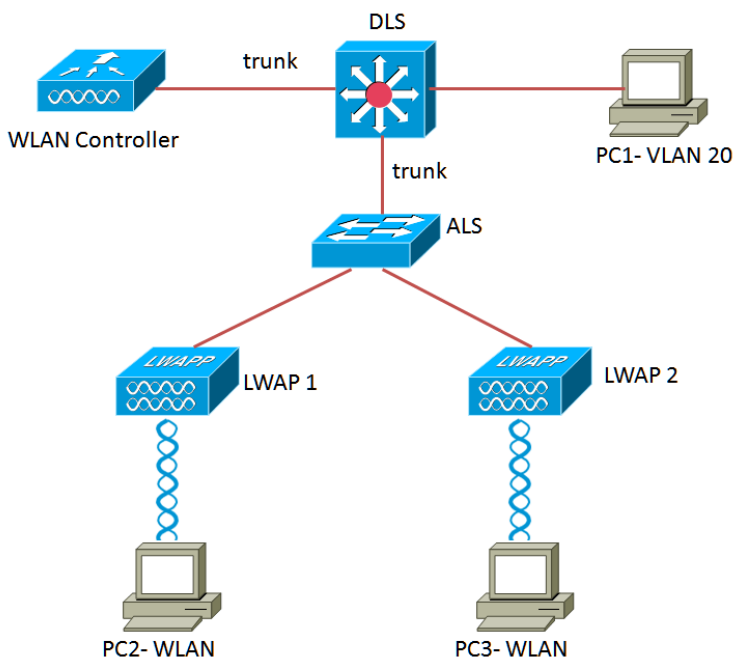
Rysunek 9.2. Autonomiczny i lekki punkt dostępu

Wraz z przebudową infrastruktury, częściowo zmieniła się rola punktów dostępu. Stałe pozostały (obsługiwane zarówno przez AP jak i LAP): obsługa kanałów dostępu, zarządzanie adresowaniem MAC i szyfrowanie. W przypadku rozwiązań ujednoczonych, funkcje związane z zarządzaniem kanałami, powiązaniem i roamingiem, uwierzytelnianiem klientów, obsługą zabezpieczeń i QoS zostały przeniesione do kontrolera bezprzewodowej sieci LAN (WLC). Zmienił się również sposób przesyłania danych. W tradycyjnym podejściu, dane z punktu dostępu przesyłane są bezpośrednio poprzez sieć (do najbliższego przełącznika). Po zastosowaniu rozwiązań ujednoczonych, cała komunikacja jest przekazywana od lekkich punktów dostępu (LAP) do kontrolera (WLC), poprzez tunel w którym następuje kapsułkowanie danych. W tunelu tym wydzielone zostały dwa kanały:

- kanał komunikatów kontroli - służący do wymiany informacji zawierających konfigurację LAP jak również informacje służące do zarządzania nim. Komunikaty te są uwierzytelnione i szyfrowane (tylko zaufane lekkie punkty dostępu (LAP) mogą połączyć się z kontrolerem i wymieniać z nim informacje),
- kanał danych - pakiety wysyłane od i do klientów bezprzewodowych powiązanych z punktem dostępu. Nie są one ani szyfrowane, ani zabezpieczane.

Dzięki zastosowaniu centralnego punktu zarządzania, uproszczony został model zarządzania siecią: z wielu niezależnych punktów z autonomicznymi konfiguracjami, do modelu w którym kontroler (WLC) pełni rolę "zarządcy", oferując następujące usługi:

- przydzielanie kanału radiowego stosowanego przez każdy z punktów bazując na informacjach od innych punktów możliwość dostosowania mocy nadajnika każdego z punktów w zależności od potrzeb elastyczny roaming klienta - dzięki centralnemu punktowi przez który przechodzą wszystkie dane (WLC) klienci mogą korzystać z roamingu,
- równoważenia obciążenia - jeżeli klient znajduje się w zasięgu dwóch punktów - WLC może zdecydować o połączeniu go z mniej używanym punktem,
- monitorowania wykorzystania częstotliwości radiowych - WLC za pośrednictwem LAP może np. zbierać informacje o aktywnych obcych AP w zakresie działania sieci z możliwością blokowania obcych połączeń,
- zarządzania bezpieczeństwem - przed pełnym powiązaniem i uzyskaniem dostępu do sieci WLAN klient może być podłączony do wirtualnej sieci celem dodatkowego potwierdzenia tożsamości.



Rysunek 9.3. Schemat topologii logicznej

9.3. Przykładowa konfiguracja kontrolera WLAN

Do wykonania zadania zostaną wykorzystane:

- dwa przełączniki (warstwy trzeciej – Cisco Catalyst 3560, jeden Cisco Catalyst 2960),
- kontroler sieci bezprzewodowej: AIR-CT2504-K9,
- dwa punkty dostępu: Cisco AIR-LAP1142N-E-K9, IOS Ver. 12.4(23c) JA2.

Przed przystąpieniem do wykonania zadania należy usunąć całą konfigurację, zarówno z przełączników (`erase startup-config`, `delete vlan.dat`), jak również z kontrolera (`clear controller`). Następnie należy zrestartować urządzenia.

Przyjmujemy następujące założenia:

- VLAN 1 – VLAN służy do zarządzania siecią i kontrolerem sieci bezprzewodowej (WLC),
- VLAN 10, 30 – sieci dla hostów (PC1, PC3) w sieci bezprzewodowej,
- VLAN 20 – sieć lokalna (PC1),
- VLAN 40 – sieć dla punktów dostępu (LWAP 1, LWAP 2).
- przełączniki obsługują VLAN 1, 10, 20, 30, 40,
- połączenia pomiędzy DLS i WLAN Controller – *trunk*,

— połączenie pomiędzy DLS i ALS – *trunk*.

Właściwa konfiguracja przygotowanej infrastruktury przebiega następująco:

1. Urządzenie DLS jest przełącznikiem warstwy 3 – w zadaniu będzie pełnił rolę routera i serwera DHCP dla poszczególnych sieci bezprzewodowych. Należy skonfigurować na nim interfejsy SVI (Switched Virtual Interface). W zadaniu zaplanowano następujące adresowanie dla sieci VLAN:

```
VLAN 1 – IP 172.16.1.0/24
VLAN 10 – IP 172.16.10.0/24
VLAN 20 – IP 172.16.20.0/24
VLAN 30 – IP 172.16.30.0/24
VLAN 40 – IP 172.16.40.0/24
```

Przełącznik DLS będzie bramą domyślną dla wszystkich sieci. Przyjęto, że adresem bramy będzie pierwszy dostępny adres dla podsieci. Przykładowa konfiguracja:

```
DLS(config)# interface vlan 1
DLS(config-if)#ip address 172.16.1.1 255.255.255.0
```

Analogicznie postępujemy dla pozostałych interfejsów.

2. Uruchomienie i skonfigurowanie serwera DHCP. Komputery PC1, PC2, PC3 otrzymają podstawową konfigurację (adres IP, adres Bramy Domyślnej itp od serwera). LWAP 1 i LWAP2 muszą otrzymać informację o dostępności Kontrolera (WLAN Controller), jak również informację, że te dane są przeznaczone dla nich.

Na początku należy wykluczyć część adresów z puli automatycznego przyznawania (zapewni to brak konfliktów ze statycznymi adresami przypisanymi w zadaniu). W przykładzie zostaną wykluczone pierwsze 100 adresów dla pierwszej podsieci. Przykładowa konfiguracja:

```
DLS(config)# ip dhcp excluded-add 172.16.1.1 172.16.1.100
```

Analogicznie dla pozostałych podsieci wykluczamy po 10 adresów. Kolejną część zadania to konfiguracja poszczególnych pul DHCP. Dla pierwszej podsieci:

```
DLS(config)#ip dhcp pool pool1
DLS(dhcp-config)#network 172.16.1.0 255.255.255.0
DLS(dhcp-config)#default-router 172.16.1.1
```

Dla podsieci 20 i 30 analogicznie.

LWAP potrzebują dodatkowych informacji. Część jest przekazywana przez dodatkową opcję: 43 – jest to tzw. *vendor-specific-option*. Daje ona do-

datkową informację do LWAP o adresie kontrolera WLAN Controller. Jest ona przedstawiona w postaci szesnastkowej w formacie TLV (*type, lenght, value*). Pierwsza część to F1 (typ), druga reprezentuje długość następnego pola. W naszym przypadku jest to 04 (adres 4-bajtowy). W tym miejscu mogą się pojawić inne opcje, np. jeżeli stosujemy więcej niż jeden kontroler. Dla dwóch kontrolerów będzie to 08, dla większej liczby analogicznie. Ostatnia część to zakodowany szesnastkowo adres IP kontrolera. Dla naszego zadania jest to adres 172.16.1.100 – szesnastkowo AC100164. Cała wartość opcji 43 to f104ac100164. Drugą dodatkową opcją jest 60. Specyfikuje ona identyfikator, jaki powinien być użyty przez AP. Korzystamy z AP CISCO Aironet 1140.

Cała konfiguracja dla VLAN 40:

```

1 DLS(dhcp-config)#ip dhcp pool pool40
  DLS(dhcp-config)#network 172.16.40.0 255.255.255.0
3 DLS(dhcp-config)#default-router 172.16.40.1
  DLS(dhcp-config)#option 43 hex f104.ac10.010a
5 DLS(dhcp-config)#option 60 ascii "Cisco AP c1140"
```

3. W zadaniu zastosowany został przełącznik warstwy 3. W celu uzyskania pełnej funkcjonalności musi na nim być uruchomiony routing.

```
DLS(config)#ip routing
```

Poniżej zaprezentowana jest przykładowa konfiguracja przełączników.

- DLS Fe0/23 - WLC Port 1 - *trunk*
- DLS Fe 0/24 - komputer testowy PC1 - VLAN 20
- DLS Fe0/8 - ALS Fe0/8 *trunk*
- ALS Fe0/23 - LWAP 1 VLAN 40
- ALS Fe0/24 - LWAP 2 VLAN 40

Listing 9.1. Istotne fragmenty pliku konfiguracyjnego przełącznika DLS

```

1 hostname DLS

3 ip routing

5 ip dhcp excluded-address 172.16.1.1 172.16.1.100
  ip dhcp excluded-address 172.16.10.1 172.16.10.10
7 ip dhcp excluded-address 172.16.20.1 172.16.20.10
  ip dhcp excluded-address 172.16.30.1 172.16.30.10
9 ip dhcp excluded-address 172.16.40.1 172.16.40.10
  !
11 ip dhcp pool pool1
    network 172.16.1.0 255.255.255.0
13   default-router 172.16.1.1
  !
```

```
15 ip dhcp pool pool10
    network 172.16.10.0 255.255.255.0
17     default-router 172.16.10.1
    !
19 ip dhcp pool pool20
    network 172.16.20.0 255.255.255.0
21     default-router 172.16.20.1
    !
23 ip dhcp pool pool30
    network 172.16.30.0 255.255.255.0
25     default-router 172.16.30.1
    !
27 ip dhcp pool pool40
    network 172.16.40.0 255.255.255.0
29     default-router 172.16.40.1
    option 43 hex f104.ac10.0164
31     option 60 ascii "Cisco AP c1140"
    !
33 !
    interface FastEthernet0/8
35     switchport trunk encapsulation dot1q
    switchport mode trunk
37 !
    !
39 interface FastEthernet0/23
    switchport trunk encapsulation dot1q
41     switchport mode trunk
    !
43 interface FastEthernet0/24
    switchport access vlan 20
45     switchport mode access
    spanning-tree portfast
47 !
    interface Vlan1
49     ip address 172.16.1.1 255.255.255.0
    !
51 interface Vlan10
    ip address 172.16.10.1 255.255.255.0
53 !
    interface Vlan20
55     ip address 172.16.20.1 255.255.255.0
    !
57 interface Vlan30
    ip address 172.16.30.1 255.255.255.0
59 !
    interface Vlan40
61     ip address 172.16.40.1 255.255.255.0
    !
```

Listing 9.2. Istotne fragmenty pliku konfiguracyjnego przełącznika ALS

```

hostname ALS
2 !
interface FastEthernet0/8
4  switchport trunk encapsulation dot1q
   switchport mode trunk
6
interface FastEthernet0/23
8  switchport access vlan 40
   switchport mode access
10 spanning-tree portfast
   !
12 interface FastEthernet0/24
   switchport access vlan 40
14  switchport mode access
   spanning-tree portfast
16 !

```

9.4. Konfiguracja kontrolera WLAN z użyciem wiersza poleceń

Przy pierwszym uruchomieniu kontrolera, kreator konfiguracji pomoże przejść przez proces wstępnej konfiguracji urządzenia. Opcje domyślne zostały zaprezentowane w nawiasach kwadratowych []. Jeżeli do wyboru jest więcej niż jedna opcja – domyślną jest opcja opisana dużymi literami.

```

(Cisco Controller)
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup

```

Należy wyłączyć automatyczną instalację:

```
Would you like to terminate autoinstall? [yes]:
```

Nadajemy nazwę dla urządzenia "cisco":

```
System Name [Cisco_e2:56:44] (31 characters max): cisco
```

Konfigurujemy hasło i nadajemy nazwę użytkownika:

```
Enter Administrative User Name (24 characters max): cisco
Enter Administrative Password (3 to 24 characters): *****
Re-enter Administrative Password                : *****

```

Kolejnym krokiem jest konfiguracja interfejsu służącego do zarządzania, wraz z bramą domyślną.

```
Management Interface IP Address: 172.16.1.100
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 16 72.16.1.1
```

Ponieważ kontroler jest połączony z przełącznikiem DLS przy użyciu łącza *trunk*, musimy zdecydować jaki ma być identyfikator (oznaczenie) sieci VLAN na połączeniu. W naszym przypadku jest to VLAN 1 domyślnie jest on nieoznakowany (*native* 802.1q VLAN)

Do komunikacji z interfejsem kontrolera będzie wykorzystywany port 1.

```
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
```

Wskazujemy adres serwera DHCP:

```
Management Interface DHCP Server IP Address: 172.16.1.1
```

Konfigurujemy wirtualny adres IP bramy (jest to fikcyjny adres wykorzystywany np. przy zarządzaniu bezpieczeństwem przez warstwę 3.):

```
Virtual Gateway IP Address: . 1.1.1.1
```

Konfigurowanie grupy mobilnej, nadanie nazwy dla sieci, umożliwienie używania statycznych adresów w sieci i konfiguracja serwera Radius:

```
Mobility/RF Group Name: umcs
Network Name (SSID): umcs
Configure DHCP Bridging Mode [yes][NO]:
Allow Static IP Addresses [YES][no]:
```

Ustalenie kodu kraju (związane jest to z zakresami częstotliwości dopuszczonymi w poszczególnych krajach (Rozdział 2):

```
Enter Country Code list (enter 'help'
for a list of countries) [US]: PL
Pozostałe ustawienia pozostawiamy domyślne:
\begin{lstlisting}[numbers=none]
Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:
```

Zapisujemy konfigurację, urządzenie restartuje się:

```
Configuration correct? If yes, system will save it
```

```
and reset . [yes][NO]: yes
```

```
Configuration saved!
```

```
Resetting system with new configuration...
```

Po restarcie i zalogowaniu powinno się zmienić znak zgłoszenia:

```
Enter User Name (or 'Recover-Config' this one-time only  
to reset configuration to factory defaults)
```

```
User: cisco
```

```
Password:*****
```

```
(Cisco Controller) >config prompt WSKK_CONTROLLER  
(WSKK_CONTROLLER)>
```

Następnie zapewnić dostęp do kontrolera poprzez Telnet i HTTP:

```
(WSKK_CONTROLLER) >config network telnet enable
```

```
(WSKK_CONTROLLER) >config network webmode enable
```

Została wykonana wstępna konfigurację kontrolera. Konfigurację można kontynuować przez przeglądarkę WWW.

9.5. Konfigurowanie kontrolera WLAN przez przeglądarkę WWW

Celem tej części jest zaprezentowanie przykładowej konfiguracji nowej sieci bezprzewodowej na kontrolerze WLAN.

1. Należy sprawdzić, czy komputer (PC1) uzyskał poprawny adres z serwera dhcp i czy możliwe jest nawiązanie komunikacji z interfejsem kontrolera (rys. 9.4).
2. Otwieramy w przeglądarce stronę WWW kontrolera (rys. 9.5). Używamy nazwy użytkownika i hasła skonfigurowanego w poprzednim rozdziale.
3. Po zalogowaniu się zostajemy przeniesieni na zakładkę Monitor. (rys. 9.6). Możemy z niej odczytać informacje o typie kontrolera, liczbie punktów dostępu wspieranych przez niego, adresie IP interfejsu do zarządzania, wersji oprogramowania itp. Z prawej strony ekranu znajdują się informacje o obcych (ang. *rogue*) punktach dostępu wraz z informacją o ich klientach.

```

C:\> Wiersz polecenia
Konfiguracja IP systemu Windows

Karta Ethernet Cisco Lab:

    Sufiks DNS konkretnego połączenia :
    Adres IP. . . . . : 172.16.20.12
    Maska podsieci. . . . . : 255.255.255.0
    Brama domyślna. . . . . : 172.16.20.1

C:\Documents and Settings\XPMUser>ping 172.16.1.100

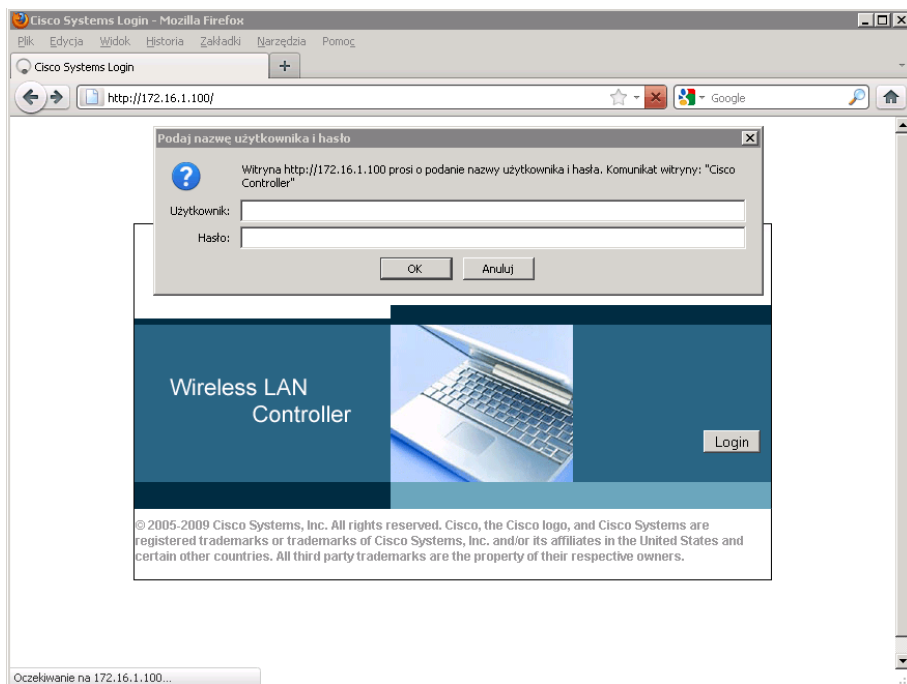
Badanie 172.16.1.100 z użyciem 32 bajtów danych:

Odpowiedź z 172.16.1.100: bajtów=32 czas=2ms TTL=127
Odpowiedź z 172.16.1.100: bajtów=32 czas<1 ms TTL=127
Odpowiedź z 172.16.1.100: bajtów=32 czas=1ms TTL=127
Odpowiedź z 172.16.1.100: bajtów=32 czas=1ms TTL=127

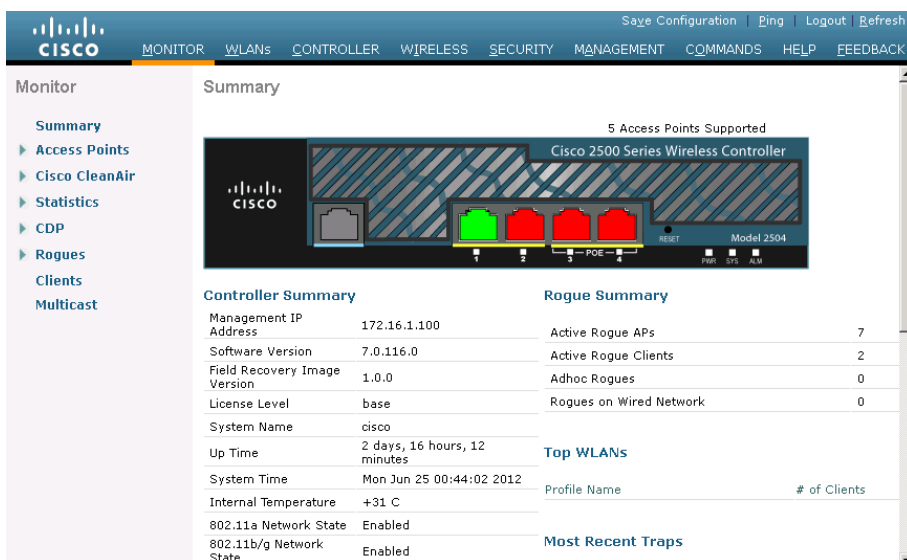
Statystyka badania ping dla 172.16.1.100:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
    Szacunkowy czas błędzenia pakietów w millisekundach:
        Minimum = 0 ms, Maksimum = 2 ms, Czas średni = 1 ms
  
```

Rysunek 9.4. Konfiguracja IP komputera PC1, wraz z testem łączności

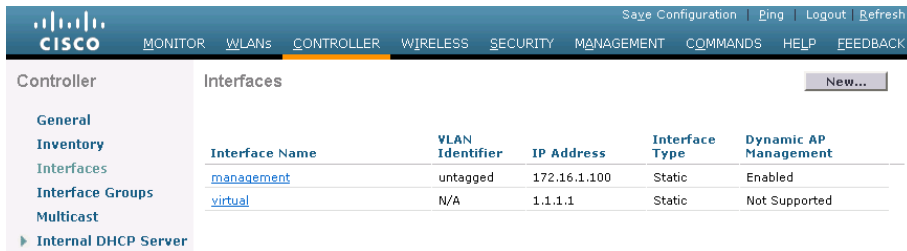
4. Przechodzimy do zakładki Controller, link Interfaces. wyświetlone są dwa interfejsy skonfigurowane w trybie linii poleceń (rys. 9.7). Należy skonfigurować nowy interfejs dla stworzenia nowej sieci bezprzewodowej (wykorzystywanej przez hosty podłączone do naszych AP), wybierając opcję New. W naszym przypadku nowy interfejs nazywamy UMCS, przypisujemy mu VLAN 10 (rys. 9.8).
5. Wybieramy nowo utworzony interfejs i konfigurujemy go (rys. 9.9). Musimy ustawić: numer portu przez który będą przepływały dane (1), identyfikator sieci VLAN (10) i adresy kontrolera, bramy domyślnej i serwera dhcp. Po wykonaniu zadania na liście interfejsów pojawi się nowy: rys. 9.10. Należy go uaktywnić.
6. Przechodzimy do zakładki WLANs, tworzymy nowy profil dla sieci bezprzewodowej – rys. 9.11. Nazywamy ją np. UMCS, nadajemy SSID (w naszym przypadku również UMCS). Po wykonaniu tego kroku nowy profil pojawi się na liście profili (rys. 9.12). Otwieramy jego właściwości, zaznaczamy pole Enable, wybieramy interfejs UMCS, określamy opcję rozgłaszania SSID) – rys. 9.13.
7. Konfigurujemy zasady bezpieczeństwa dla nowo powstałej sieci (w naszym przypadku sieć będzie niezabezpieczona) – rys. 9.14.
8. Po poprawnym przejściu wszystkich punktów sprawdzamy dostępność sieci. Jest wśród nich nowo utworzona sieć UMCS – rys. 9.15.
9. Łączymy się z siecią i sprawdzamy adres IP naszego połączenia – rys. 9.16. Nasz klient otrzymał adres z podsieci przeznaczonej dla niego.



Rysunek 9.5. Strona startowa kontrolera wraz z oknem logowania



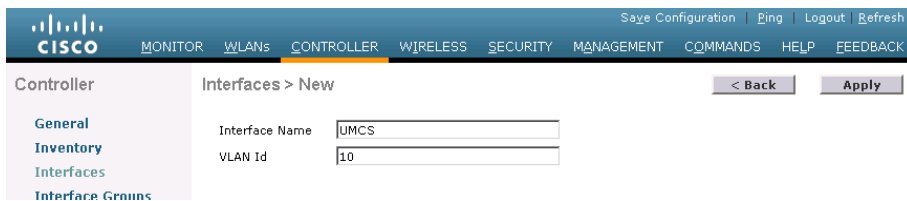
Rysunek 9.6. Widok strony kontrolera po zalogowaniu



The screenshot shows the Cisco Controller configuration page for the 'CONTROLLER' section, specifically the 'Interfaces' tab. A table lists the configured interfaces:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	untagged	172.16.1.100	Static	Enabled
virtual	N/A	1.1.1.1	Static	Not Supported

Rysunek 9.7. Okno konfiguracji interfejsów

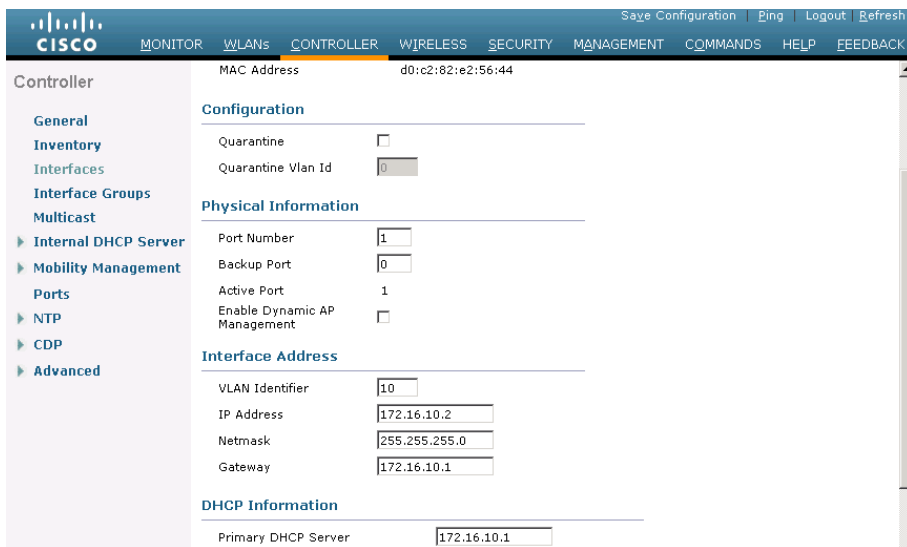


The screenshot shows the 'New' interface configuration page in the Cisco Controller. The form fields are:

- Interface Name:
- VLAN Id:

Buttons for '< Back' and 'Apply' are visible at the bottom right.

Rysunek 9.8. Dodawanie nowego interfejsu



The screenshot shows the detailed configuration page for a new interface. The MAC Address is 'd0:c2:82:e2:56:44'. The configuration is divided into several sections:

- Configuration:**
 - Quarantine:
 - Quarantine Vlan Id:
- Physical Information:**
 - Port Number:
 - Backup Port:
 - Active Port: 1
 - Enable Dynamic AP Management:
- Interface Address:**
 - VLAN Identifier:
 - IP Address:
 - Netmask:
 - Gateway:
- DHCP Information:**
 - Primary DHCP Server:

Rysunek 9.9. Konfiguracja interfejsu

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	untagged	172.16.1.100	Static	Enabled
umcs	10	172.16.10.2	Dynamic	Disabled ▼
virtual	N/A	1.1.1.1	Static	Not Supported

Rysunek 9.10. Okno interfejsów

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	cnppod	cnppod	Enabled	[WPA2][Auth(802.1X)]

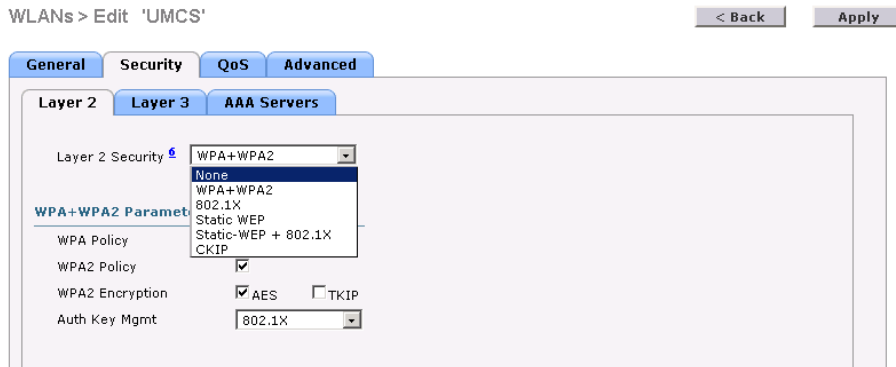
Rysunek 9.11. Tworzenie nowego profilu sieci bezprzewodowej

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	cnppod	cnppod	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	UMCS	UMCS	Disabled	[WPA2][Auth(802.1X)]

Rysunek 9.12. Nowy profil na liście profili WLAN

Profile Name	UMCS
Type	WLAN
SSID	UMCS
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	umcs
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Rysunek 9.13. Ogólne ustawienia profilu



Rysunek 9.14. Ustawienia zabezpieczeń sieci



Rysunek 9.15. Lista dostępnych sieci bezprzewodowych

```
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . . :
IPv4 Address. . . . . : 172.16.10.11
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.10.1
```

Rysunek 9.16. Konfiguracja IP klienta podłączonego do sieci z SSID UMCS

9.6. Zadanie

Postępując w analogiczny do zaprezentowanego stwórz nową sieć (przy-
pisz ją do wolnego VLAN) i zabezpiecz jej działanie protokołem WPA2.

ROZDZIAŁ 10

ROZWIĄZANIA TYPU *open source* DLA SIECI BEZPRZEWODOWYCH

10.1. Wstęp	118
10.2. Możliwości alternatywnego oprogramowania	119

10.1. Wstęp

Routerzy bezprzewodowe, przeznaczone do użytku domowego, z zasady są łatwe do skonfigurowania. Posiadają przyjazny interfejs graficzny. W niektórych przypadkach, proces konfiguracji sieci bezprzewodowej (wraz z mechanizmami bezpieczeństwa) może być niemal całkowicie zautomatyzowany i możliwy do przeprowadzenia przez użytkownika nieposiadającego wiedzy technicznej, dzięki dołączonemu oprogramowaniu instalacyjnemu. Jednocześnie jednak liczba dostępnych opcji konfiguracyjnych, chociaż w zupełności wystarczająca przeciętnemu użytkownikowi, jest bardzo niewielka w porównaniu z urządzeniami profesjonalnymi.

W 2003 roku ujawniono fakt wykorzystywania w oprogramowaniu urządzeń firmy Linksys (wiodącego wówczas producenta urządzeń sieciowych segmentu SOHO, obecnie marka Cisco) fragmentów kodu Linuksa [39]. Zgodnie z licencją GPL, zmusiło to firmę do publikacji kodu źródłowego urządzeń WRT54G. To z kolei zapoczątkowało wiele projektów, mających na celu opracowanie poprawionych wersji, wyposażonych w dodatkowe funkcje. Najbardziej znane z nich to HyperWRT oraz oprogramowanie firmy Sveasoft. Ciągłe jednak większość kodu pochodziła z oryginalnego źródła. Z kolei firma Sveasoft wprowadziła opłaty za korzystanie ze swojego systemu.

Te fakty zmotywowały programistów do stworzenia nowego oprogramowania na licencji GNU GPL, bazującego na jądrze Linuksa, od podstaw, a nie poprzez modyfikację kodów Linksysa [40]. Dwa prawdopodobnie najbardziej znane i do tej pory rozwijane projekty z tej grupy to DD-WRT¹ i OpenWRT². Powstało również wiele innych, samodzielnych lub na bazie wymienionych, np. DebWRT, Tomato, FreeWRT, RouterTech.Org.

Alternatywne systemy umożliwiają dostęp do zwykłego wiersza poleceń Linuksa. Na routerze można instalować dodatkowe pakiety oprogramowania, wzbogacając go o nowe możliwości. Można też wykorzystać go jako miniaturowy komputer, do zupełnie innych celów niż te, do których został zaprojektowany. Jednocześnie, przyjazny interfejs graficzny dostępny poprzez przeglądarkę WWW sprawia, że stopień trudności przeprowadzenia standardowej konfiguracji znacząco nie odbiega od oryginalnego oprogramowania.

Początkowo alternatywne oprogramowanie powstało tylko dla routera WRT54G i podobnych. Obecnie jego instalacja jest możliwa na bardzo wielu urządzeniach różnych producentów. Listy routerów przetestowanych pod kątem zgodności są na bieżąco aktualizowane na stronach WWW poszczególnych projektów. Negatywną konsekwencją zmiany oprogramowania jest natomiast utrata gwarancji oraz ryzyko zablokowania lub nawet trwałego

¹ <http://www.dd-wrt.com/>

² <https://openwrt.org/>

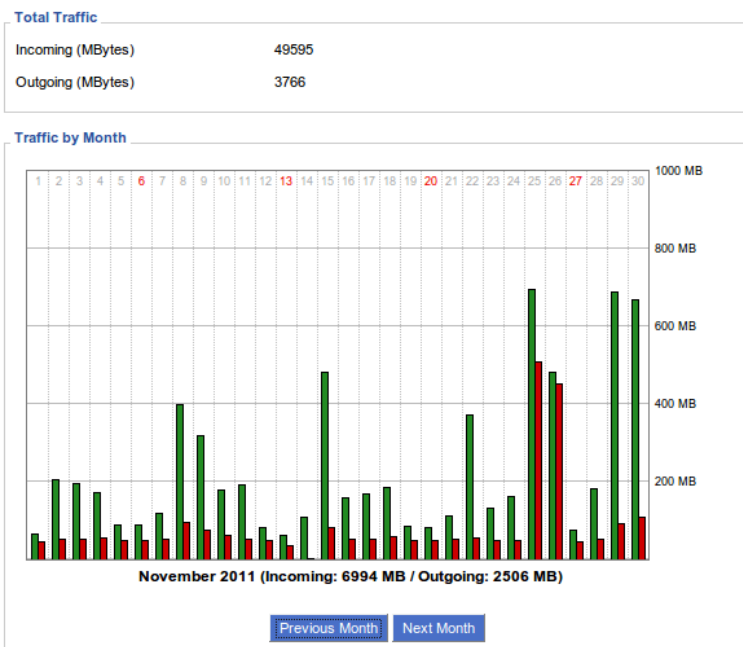
uszkodzenia urządzenia, w razie niepowodzenia operacji. Aby je ograniczyć, należy ściśle przestrzegać zalecanej procedury instalacji dla danego modelu. Istnieje też możliwość zakupu routera z zainstalowaną już przez producenta, zazwyczaj lekko zmodyfikowaną, wersją alternatywnego oprogramowania (np. DD-WRT).

10.2. Możliwości alternatywnego oprogramowania

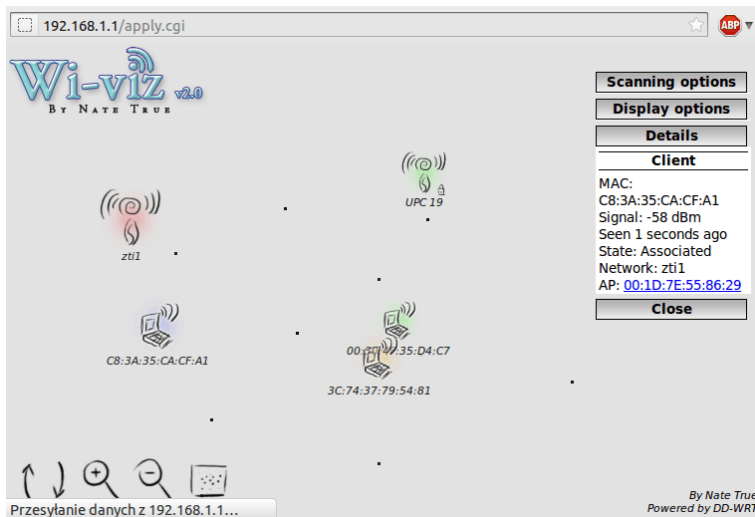
Możliwości alternatywnego oprogramowania zostaną przedstawione na przykładzie DD-WRT v24, przy czym ze względu na liczbę dostępnych funkcji, krótko omówione będą tylko niektóre. Wiele spośród nich jest często spotykanych w urządzeniach profesjonalnych. Możliwe jest więc uzyskanie zaawansowanych funkcjonalności, bardzo niskim kosztem. DD-WRT jest obecnie dostępne w kilkunastu wariantach, różniących się możliwościami i wymaganiami sprzętowymi.

Najciekawsze funkcje to między innymi:

- konfiguracja sieci VLAN i połączeń trunk (802.1q),
- możliwość skonfigurowania wirtualnych interfejsów radiowych i jednoczesnego uruchomienia kilku SSID z różnymi ustawieniami,
- kilkanaście języków interfejsu, do wyboru,
- uwierzytelnianie w protokole 802.1x EAP,
- możliwość skonfigurowania ograniczeń dostępu do sieci na podstawie różnorodnych kryteriów,
- tryb izolacji klientów, uniemożliwiający transmisję między hostami w sieci bezprzewodowej, często stosowany w publicznych hotspotach,
- tryb klienta – odpowiednik mostu grupy roboczej (Rozdział 8),
- bezprzewodowy system dystrybucyjny,
- możliwość pracy w roli repeatera bezprzewodowego,
- różnorodne opcje konfiguracyjne DHCP i DNS,
- oprogramowanie umożliwiające łatwe skonfigurowanie darmowego lub płatnego hotspota,
- strefa zdemilitaryzowana (DMZ),
- wsparcie dla IPv6,
- system plików JFFS (*Journalling Flash File System*), umożliwiający przechowywanie na routerze wszelkich danych i oprogramowania,
- wsparcie dla sieciowych systemów plików (np. Samba), umożliwiające między innymi udostępnienie w sieci dysku USB dołączonego do routera,
- obsługa kart MMC/SD, przy czym mogą być wymagane niewielkie zmiany sprzętowe (np. wlutowanie gniazda),
- możliwość monitorowania ruchu oraz uzyskiwania różnorodnych statystyk – rys. 10.1,



Rysunek 10.1. Informacje statystyczne o ruchu sieciowym

Rysunek 10.2. Przegląd sieci bezprzewodowej (*site survey*)

- klient i serwer OpenVPN oraz PPTP, umożliwiające tworzenie tuneli VPN,
- przekazywanie portów (*port forwarding*),

- wiele mechanizmów QoS (*Quality of Service*), umożliwiających zapewnienie odpowiedniego pasma sieciowego dla określonych użytkowników lub protokołów, wsparcie dla aplikacji multimedialnych,
- routing z wykorzystaniem między innymi protokołów RIP, OSPF, BGP,
- możliwość lokalnego lub zdalnego przechowywania logów systemowych (syslog),
- możliwość przeprowadzenia przeglądu sieci bezprzewodowej (ang. *site survey*) – rys. 10.2,
- klient i serwer SSH,
- możliwość edycji skryptów startowych,
- możliwość ustawienia mocy nadajnika, w szerokim zakresie.

W razie braku potrzebnej funkcjonalności, zwykle można ją uzyskać poprzez modyfikację skryptów, napisanie własnych, lub instalację dodatkowego oprogramowania. Można również stworzyć własną dystrybucję DD-WRT, zawierającą tylko potrzebne pakiety, korzystając z narzędzia *Firmware Modification Kit*. Dzięki temu zazwyczaj nie ma konieczności samodzielnej re-kompilacji kodu źródłowego, nawet w przypadku niestandardowych potrzeb.

DODATEK A

DHCP I TRANSLACJA ADRESÓW

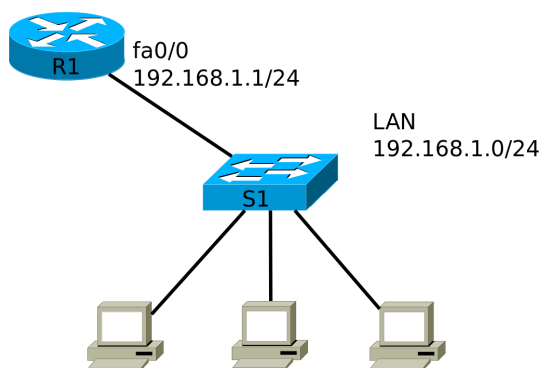
A.1. DHCP	124
A.2. Translacja adresów	125

A.1. DHCP

Znaczna część urządzeń Cisco, wyposażonych w system operacyjny IOS (routery, przełączniki Ethernet, bezprzewodowe punkty dostępowe), może dodatkowo pełnić rolę serwera DHCP. Jeżeli usługa ta jest dostępna, domyślnie jest włączona. W razie potrzeby, można natomiast serwer DHCP wyłączyć poleceniem:

```
no service dhcp
```

w trybie konfiguracji globalnej.



Rysunek A.1. Sieć z serwerem DHCP

Poniżej przedstawiony jest przykład konfiguracji routera R1 z rys. A.1, tak aby pełnił rolę serwera DHCP dla dołączonej do niego sieci LAN. Zakładamy, że interfejs FastEthernet0/0 routera jest włączony i ma skonfigurowany adres IP.

1. Niektóre adresy powinny zostać wykluczone z puli adresów IP, którą dysponuje serwer DHCP: statycznie przypisane adresy urządzeń sieciowych, serwerów itp. W naszym przypadku jest to adres interfejsu routera. Wykluczenia dokonujemy poleceniem:

```
ip dhcp excluded-address 192.168.1.1
```

w trybie konfiguracji globalnej. W razie podania dwóch adresów jako parametry, wykluczony zostanie cały przedział.

2. Tworzymy pulę adresów o dowolnej nazwie (np. *PULA1*), a następnie podajemy adres podsieci, z której będą przydzielane adresy oraz adres bramy domyślnej dla hostów:

```
ip dhcp pool PULA1
network 192.168.1.0 255.255.255.0
```

```
default-router 192.168.1.1
```

Jeżeli dysponujemy serwerem DNS, podajemy również informację o jego adresie:

```
dns-server adresIP
```

Dostępnych jest także wiele innych, opcjonalnych parametrów konfiguracyjnych, np. czas dzierżawy adresu. W razie gdy serwer DHCP ma obsługiwać kilka sieci, dla każdej z nich należy stworzyć oddzielną pulę adresów. W momencie przydzielania adresu IP, serwer automatycznie wybierze pulę odpowiednią dla sieci, w której znajduje się host wysyłający żądanie.

3. Jeżeli komputery z sieci lokalnej zostaną skonfigurowane tak, aby ustawienia IP były pozyskiwane automatycznie, powinny otrzymać je od serwera DHCP działającego na routerze R1. Informacje o adresach, które zostały przydzielone przez serwer, wyświetla polecenie:

```
show ip dhcp binding
```

Serwer DHCP może przydzielać adresy IP także interfejsom (fizycznym i wirtualnym) urządzeń sieciowych Cisco. W trybie konfiguracji takiego interfejsu należy użyć polecenia:

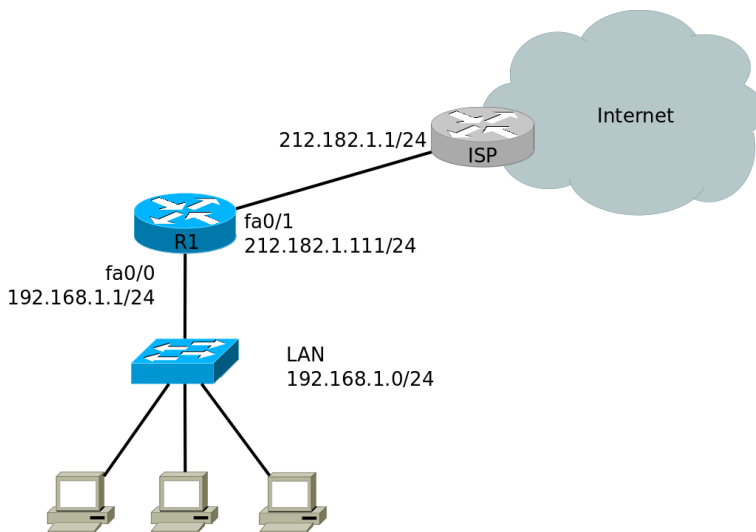
```
ip address dhcp
```

A.2. Translacja adresów

Jeżeli w sieci korzysta się z prywatnych adresów IP (RFC 1918 [41]), które nie mogą występować w publicznym Internecie, mechanizm translacji adresów (ang. *Network Address Translation*, NAT) pozwala hostom na dostęp do Internetu [42]. Przedstawiony jest tu sposób konfiguracji tylko jednego z wariantów translacji adresów, w którym dysponując jednym publicznym adresem IP, chcemy umożliwić wielu komputerom z sieci prywatnej jednoczesny dostęp do sieci zewnętrznej. Ta sytuacja jest określana mianem przeciążonej translacji adresów (*NAT overload*, *Port Address Translation – PAT* lub *IP masquerading*).

Załóżmy, że router R1 z rys. A.2 łączy sieć lokalną z Internetem i będzie wykonywał translację adresów. Ma już skonfigurowane interfejsy sieciowe oraz statyczną trasę domyślną do ISP:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 212.182.1.1
```



Rysunek A.2. Przykład zastosowania translacji adresów

Adres 212.182.1.111, przypisany interfejsowi fa0/1, jest jedynym publicznym adresem IP, jakim dysponujemy.

1. Musimy wskazać interfejs łączący z siecią wewnętrzną (z adresowaniem prywatnym) oraz zewnętrzną (Internetem):

```
interface fa0/0
  ip nat inside
interface fa0/1
  ip nat outside
```

2. Tworzymy listę kontroli dostępu (ACL) określającą adresy, które będą podlegały translacji. Zakładamy, że dostęp do Internetu mają uzyskać wszystkie hosty z sieci 192.168.1.0/24:

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

3. Włączamy translację adresów:

```
ip nat inside source list 1 interface fastEthernet 0/1
  overload
```

“1” jest tu numerem listy ACL skonfigurowanej powyżej, natomiast fastEthernet0/1 – nazwą interfejsu zewnętrznego, którego adres będzie wykorzystywany jako źródłowy, dla pakietów wysyłanych z sieci lokalnej do Internetu.

Działanie translacji adresów można zweryfikować poleceniem:

```
show ip nat translations
```

Przykładowo, po wydaniu na jednym z komputerów w sieci lokalnej (o adresie IP 192.168.1.77) polecenia:

```
ping 212.182.1.1
```

otrzymamy wynik zbliżony do następującego:

```
R1#show ip nat translations
Pro  Inside global    Inside local    [...] Outside global
icmp 212.182.1.111:1  192.168.1.77:1 [...] 212.182.1.1:1
icmp 212.182.1.111:2  192.168.1.77:2 [...] 212.182.1.1:2
icmp 212.182.1.111:3  192.168.1.77:3 [...] 212.182.1.1:3
icmp 212.182.1.111:4  192.168.1.77:4 [...] 212.182.1.1:4
```

Zgodnie z powyższą tabelą, w pakietach wysyłanych przez router do Internetu (z adresem docelowym 212.182.1.1, zewnętrznym), wewnętrzny adres lokalny (*Inside local*) 192.168.1.77 jest zastępowany publicznym, wewnętrznym globalnym (*Inside global*) 212.182.1.111.

BIBLIOGRAFIA

- [1] IEEE, *IEEE 802.5 Web Site*, <http://www.ieee802.org/5/www8025org/>.
- [2] ANSI X3T9.5 Committee, *FDDI Station Management (SMT)*, Rev. 6.1, March 15 1990.
- [3] ARCNET Trace Association, *ATA 878.1 - 1999 Local Area Network: Token Bus*, 1999, <http://www.arcnet.com>.
- [4] K. Kuczyński, R. Stęgiński, *Routing w sieciach IP*, UMCS, Lublin 2011.
- [5] R. Graziani, A. Johnson, *Akademia sieci Cisco. CCNA Exploration. Semestr 2. Protokoły i koncepcje routingu*, PWN 2011.
- [6] K. Kuczyński, W. Suszyński, *Przełączanie w sieciach lokalnych*, UMCS, Lublin 2012.
- [7] W. Lewis, *Akademia sieci Cisco. CCNA Exploration. Semestr 3. Przełączanie sieci LAN i sieci bezprzewodowe*, PWN, 2011.
- [8] D. Hucaby, *CCNP Switch. Oficjalny przewodnik certyfikacji*, Wydawnictwo Naukowe PWN, 2012.
- [9] J. Ross, *Sieci bezprzewodowe. Przewodnik po sieciach Wi-Fi i szerokopasmowych sieciach bezprzewodowych*, wydanie II, Helion, 2009.
- [10] M.S. Gast, *802.11. Sieci bezprzewodowe. Przewodnik encyklopedyczny*, seria O'Reilly, Helion, 2003.
- [11] B.Potter, B. Fleck, *802.11. Bezpieczeństwo*, seria O'Reilly, Helion, 2004.
- [12] R. Pejman, L. Jonathan, *Bezprzewodowe sieci LAN 802.11. Podstawy*, Wydawnictwo Naukowe PWN, 2007.
- [13] M. Gast, *802.11n: A Survival Guide*, O'Reilly Media, Inc, USA, 2012.
- [14] E. Perahia, R. Stacey, *Next Generation Wireless LANs: Throughput, Robustness, and Reliability in 802.11n*, Cambridge University Press, 2008.
- [15] B. Henry, *CCIE Security. Oficjalny Podręcznik Przygotowujący do Egzaminu*, Wydawnictwo Naukowe PWN, 2004.
- [16] IEEE, *Standard 802.11-2012*, <http://standards.ieee.org/findstds/standard/802.11-2012.html>.
- [17] IEEE, *Standard 802.16-2009*, <http://standards.ieee.org/getieee802/download/802.16-2004.pdf>.
- [18] IEEE, *Standard 802.11f-2003*, <http://standards.ieee.org/getieee802/download/802.11F-2003.pdf>.
- [19] IEEE, *Standard 802.2-1998*, <http://standards.ieee.org/getieee802/download/802.2-1998.pdf>.
- [20] IEEE, *Standard 802.11b-1999*, <http://standards.ieee.org/getieee802/download/802.11b-1999.pdf>.

- [21] IEEE, *Standard 802.11a-1999*, <http://standards.ieee.org/getieee802/download/802.11a-1999.pdf>.
- [22] IEEE, *Standard 802.11g-2003*, <http://standards.ieee.org/getieee802/download/802.11g-2003.pdf>.
- [23] IEEE, *Standard 802.11n-2009*, <http://standards.ieee.org/getieee802/download/802.11n-2009.pdf>.
- [24] IEEE, *Standard 802.3-2008*, <http://standards.ieee.org/about/get/802/802.3.html>.
- [25] IEEE, *Standard 802.11-2007*, <http://standards.ieee.org/about/get/>.
- [26] Cisco Systems, *Password Recovery Procedure for Cisco Aironet Equipment*, Document ID: 9215, <http://www.cisco.com/image/gif/paws/9215/pwrec-2.pdf>.
- [27] Cisco Systems, *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, Versions 12.4(10b)JA and 12.3(8)JEC*, http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/command/reference/cr12410b.pdf.
- [28] Cisco Systems, *Cisco Guide to Harden Cisco IOS Devices*, Document ID: 13608, <http://www.cisco.com/image/gif/paws/13608/21.pdf>.
- [29] IEEE, *Standard 802.11i-2004*, <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>.
- [30] IEEE, *Standard 802.1X-2010*, <http://standards.ieee.org/getieee802/download/802.1X-2010.pdf>.
- [31] Aircrack-ng, *Main documentation - Aircrack-ng suite*, <http://www.aircrack-ng.org/documentation.html>.
- [32] Cisco Systems, *Wi-Fi Protected Access 2 (WPA 2) Configuration Example*, Document ID: 67134, http://www.cisco.com/image/gif/paws/67134/wpa2_config.pdf.
- [33] Cisco Systems, *Using VLANs with Cisco Aironet Wireless Equipment*, Document ID: 46141, <http://www.cisco.com/image/gif/paws/46141/vlanswireless.pdf>.
- [34] Cisco Systems, *Cisco Aironet 1300 Series Outdoor Access Point/Bridge*, http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet09186a00802252e1.pdf.
- [35] Cisco Systems, *Outdoor Bridge Range Calculation Utility*, Document ID: 18860, <http://www.cisco.com/image/gif/paws/18860/outdoor-br-utility-calc.pdf>.
- [36] Cisco Systems, *Configuring Repeater and Standby Access Points and Workgroup Bridge Mode*, *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points Cisco IOS Releases 12.4(21a)JA1 and 12.3(8)JEC*, http://www.cisco.com/en/US/docs/wireless/access_point/12.4_21a_JA1/configuration/guide/scg12421aJA1-chap19-wgb-standby.pdf.
- [37] Cisco Systems, *Wireless Bridges Point-to-Point Link Configuration Example*, Document ID: 68087, http://www.cisco.com/application/pdf/paws/68087/bridges_pt_to_pt.pdf.
- [38] P. Calhoun, M. Montemurro, D. Stanley, *Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification*, Request for Com-

- ments: 5415, Network Working Group, 2009, <http://tools.ietf.org/html/rfc5415>.
- [39] A. Miklas, Linksys WRT54G and the GPL, *Linux Kernel Mailing List*, 2003, <https://lkml.org/lkml/2003/6/7/164>.
- [40] K. Kuczyński, M. Kuczyński, Oprogramowanie open source dla routerów Wi-Fi, *Systemy mobilne – od teorii do praktyki*, red. M. Miłosz, Polskie Towarzystwo Informatyczne, Warszawa 2007, 31-44.
- [41] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, *Address Allocation for Private Internets*, Request for Comments: 1918, Network Working Group, 1996, <http://tools.ietf.org/html/rfc1918>.
- [42] P. Srisuresh, M. Holdrege, *IP Network Address Translator (NAT) Terminology and Considerations*, Request for Comments: 2663, Network Working Group, 1999, <http://tools.ietf.org/html/rfc2663>.

SKOROWIDZ

- 2,4GHz, 17, 23
- 5GHz, 17, 23
- 802.11, vii, 3
- 802.11a, 23
- 802.11ac, 24
- 802.11b, 22
- 802.11f, 5
- 802.11g, 23
- 802.11i, 58
- 802.11n, 24
- 802.1q, 76
- 802.1x, 59
- 802.2, 34
- 802.3, 29

- access point, 3, 40
- ACK, 30
- ACL, 126
- ad-hoc, 3
- AES, 59, 64
- Aircrack-ng, 58, 61
- Airmon-ng, 61
- Airodump-ng, 61
- Aironet, viii, 41
- Aironet extensions, 90
- amplituda, 10
- antena, 13
- antena dipolowa, 15
- antena dookólna, 13
- antena izotropowa, 13
- antena kierunkowa, 13, 14, 88
- antena panelowa, 17
- antena paraboliczna, 17
- antena reflektorowa, 17
- antena Yagi, 16
- ARCNET, vii
- Association ID, 6

- Bluetooth, 2, 18
- bridge, 86
- Broadcast SSID, 45
- BSS, 3
- BSSID, 3, 34
- BVI, 44

- CAPWAP, 101
- Catalyst, viii
- CCK, 22
- CCMP, 59
- charakterystyka kierunkowa anteny, 13
- CSMA/CA, 22, 30
- CSMA/CD, 29
- CTS, 31
- częstość kołowa, 10
- częstotliwość, 10

- długość fali, 11
- dB, 12
- dBd, 15
- dBi, 14
- DCF, 30
- DD-WRT, 118
- decybel, 12
- DES, 59
- DFS, 19
- DHCP, 42, 124
- DMZ, 119
- DS, 34
- DSSS, 22
- DTP, 77

- EAP, 59, 68
- EIRP, 16
- ESS, 4
- Ethernet, vii, 2, 28, 86

- bezprzewodowy Ethernet, 28
- fala elektromagnetyczna, 10

- FDDI, vii
- filtrowanie adresów MAC, 57
- fragmentacja, 31

- gigaherc, 10
- GPRS, 2
- GSM, 2
- guest mode, 52, 57

- herc, 10
- hotspot, 48
- HyperWRT, 118

- IAPP, 5
- IBSS, 3
- IEEE, vii, 7
- infrastructure mode, 3
- interfejs BVI, 44
- IP masquerading, 125
- IPsec, 58
- IPv6, 119
- IrDA, 2, 22
- ISM, 17
- ISO/OSI, 7, 22, 28
- iwlist, 72

- jam signal, 29

- kanal radiowy, 18, 46
- Kismet, 73
- kontroler sieci bezprzewodowej, 40

- LAN, vii, 2
- LEAP, 59, 67
- lekki punkt dostępowy, 40
- lightweight access point, 40
- Linksys, 118
- Linux, 118
- LLC, 7, 34
- logo Wi-Fi, 2
- LTE, 2
- LWAPP, 101

- MAC, 7, 28
- MAN, 2
- megaherc, 10
- miliwat, 11
- MIMO, 24

- moc, 11
- model ISO/OSI, 7, 22, 28
- modulacja, 11
- monitorowanie sieci, 72
- most bezprzewodowy, 13, 86, 87
- most główny, 93
- most grupy roboczej, 87

- NAT, 125
- natywny VLAN, 77
- non-root bridge, 93

- OFDM, 23
- okres fali, 10
- OpenWRT, 118
- OSI, 7, 22, 28
- otwarte uwierzytelnianie, 58

- PAN, 2
- pasmo analogowe, 11
- pasmo cyfrowe, 11
- PAT, 125
- PHY, 7, 22
- polaryzacja, 11, 13
- prędkość światła, 11
- przełączanie przezroczyste, 34
- przełącznik bezprzewodowy, 86
- przycisk Mode, 41
- punkt dostępowy, 3, 40

- Radio0-802.11G, 42
- RADIUS, 59
- Radius, 67
- ramka 802.11, 32
- RC4, 58
- repeater, 86
- RMON, 72
- roaming, 4
- rodzimy VLAN, 77
- root bridge, 93
- router bezprzewodowy, 40, 118
- rozgłaszanie SSID, 57
- RTS, 31

- Samba, 119
- seamless roaming, 5
- sieci wirtualne, 76
- site survey, 121

SNMP, 72
SSID, 3, 45
strefa Fresnela, 90
Sveasoft, 118
system dystrybucyjny, 34
szerokość pasma, 11

TKIP, 58
Token Ring, vii
TPC, 19
translacja adresów, 125
transmitter, 34
trunk, 76
tryb gościnny, 57

UKF, 11
ukryty węzeł, 30
UMTS, 2
ustawienia fabryczne, 41

VLAN, 76
VoIP, 5

WAN, 2, 88
wat, 11
WECA, 3, 28
WEP, 58, 59
WGB, 87
Wi-Fi, vii
Wi-Fi Alliance, 3, 28
WiFi, 2
wireless bridge, 87
Wireshark, 73
wirtualny LAN, 76
workgroup bridge, 87
WPA, 58
WPA-PSK, 59
WPA2, 58
WPA2 Enterprise, 67
WPA2 Personal, 63
WPA2-PSK, 59
WRT54G, 118
współdzielony klucz, 58

Yagi, 16

zysk energetyczny, 13