4 Konfigurowanie urządzeń sieci bezprzewodowych

ZAGADNIENIA

- **Z czego składa się infrastruktura sieci bezprzewodowych?**
- **W jakich trybach mogą pracować sieci bezprzewodowe?**
- **Jakie standardy dotyczą sieci bezprzewodowych?**
- **Jak skonfigurować bezprzewodową kartę sieciową?**
- **Jak skonfigurować sieć działającą w trybie ad-hoc i infrastruktury?**
- **W jaki sposób zabezpieczyć sieć bezprzewodową przed podsłuchem?**
- **Jakie standardy szyfrowania danych używane są w sieciach bezprzewodowych?**
- **Jak włączyć szyfrowanie danych w sieci bezprzewodowej?**

Łączność bezprzewodowa zdobywa coraz szersze zastosowanie, również w dziedzinie lokalnych sieci komputerowych. **Bezprzewodowa sieć lokalna WLAN** (*Wireless Local Area Network*) jest to sieć, w której połączenia między urządzeniami sieciowymi zrealizowano bez użycia przewodów. Do przesyłania danych pomiędzy urządzeniami wykorzystuje się fale radiowe. Zakres częstotliwości fal radiowych wykorzystywany w sieciach WLAN nie podlega koncesjonowaniu i dlatego można go używać bez żadnych zezwoleń. Jednak w paś-mie tym występują znaczne zakłócenia pochodzące od innych urządzeń, np. kuchenek mikrofalowych, telefonów bezprzewodowych itp. Infrastruktura sieci bezprzewodowych składa się z:

- **kart sieciowych** – najczęściej typu PCI, PCIExpress, ExpressCard, USB, PCMCIA, ale też wbudowanych w urządzenia przenośne, takie jak laptopy, smartfony, itp.;
- **punktów dostępowych** (*Access Point*) – pełnią rolę bezprzewodowych koncentratorów w sieciach pracujących w trybie infrastruktury;
- **anten**;
- **kabli, złączy** itp.

Małe sieci bezprzewodowe mogą być budowane w trybie **ad hoc** – urządzenia komunikują się bezpośrednio ze sobą, dla większych sieci przewidziano tryb **infrastruktury**, w którym urządzenia komunikują się ze sobą za pośrednictwem punktów dostępowych. Istnieje kilka standardów sieci WLAN, różniących się częstotliwościami pracy, prędkościami przesyłania danych i sposobem kodowania sygnału. Standardy te opisuje dokument IEEE802.11. Najpopularniejsze standardy sieci bezprzewodowych to:

- **802.11a** – standard wykorzystuje pasmo częstotliwości w zakresie 5,15-5,35 GHz oraz 5,725-5,825 GHz. Obejmuje 8 kanałów przeznaczonych do pracy w budynkach oraz 4 przeznaczone do pracy między dwoma punktami (*point-to-point*). Praca na wyższych częstotliwościach powoduje zmniejszenie zasięgu w porównaniu z innymi sieciami o około połowę. Maksymalna prędkość transmisji w tym standardzie wynosi 54 Mb/s. Wadą jest brak zgodności z innymi standardami.

- **802.11b** – używa pasma w częstotliwości 2,4 GHz (od 2400 do 2485 MHz), osiągając maksymalną prędkości 11 Mb/s w promieniu 46 m w pomieszczeniach zamkniętych i 96 na otwartych przestrzeniach. Pasmo częstotliwości podzielone jest na 14 kanałów o szerokości 22 MHz, częściowo zachodzących na siebie (tylko trzy kanały nie pokrywają się w swoich zakresach). W Polsce można wykorzystywać tylko kanały od 1 do 13.
- **802.11g** – standard ten używa tego samego pasma częstotliwości, co 802.11b. Umożliwia transmisję danych z prędkością 54 Mb/s. Standard ten jest w pełni zgodny z 802.11b.
- **802.11n** – w zależności od rozwiązania (zastosowanych anten) pozwala na przesyłanie plików z prędkością teoretyczną – od 150 do 600 Mb/s. Standard „n" może działać na częstotliwości zarówno 2,4 GHz, jak i 5 GHz (jednak większość urządzeń potrafi pracować tylko w paśmie 2,4 GHz). Standard obsługuje technologię **Multiple Input Multiple Output** (MIMO) wykorzystującą wiele anten do nadawania/odbioru sygnału (sygnał jest nadawany z kilku źródeł i odbierany przez kilka odbiorników). Ponadto urządzenia 802.11n potrafią wykorzystywać wiele kanałów transmisyjnych do stworzenia jednego połączenia, co teoretycznie dodatkowo zwiększa dostępną prędkość transmisji. Starsze urządzenia obsługujące jedynie standard „b" lub „g" mogą współpracować z urządzeniem działającym w standardzie „n", jednak w takiej sytuacji następuje przełączenie na wolniejsze tempo standardu „b" lub „g".

Przed przyłączeniem komputera do sieci bezprzewodowej należy skonfigurować bezprzewodową kartę sieciową. Jeżeli w sieci bezprzewodowej będzie działał serwer DHCP, to karta będzie mogła otrzymać adres IP i inne dane niezbędne do prawidłowej pracy w sieci. Jeżeli serwera DHCP w sieci nie będzie, to wszystkie dane należy przypisać karcie ręcznie.

PRZYKŁAD 4.1.

Konfigurowanie bezprzewodowej karty sieciowej

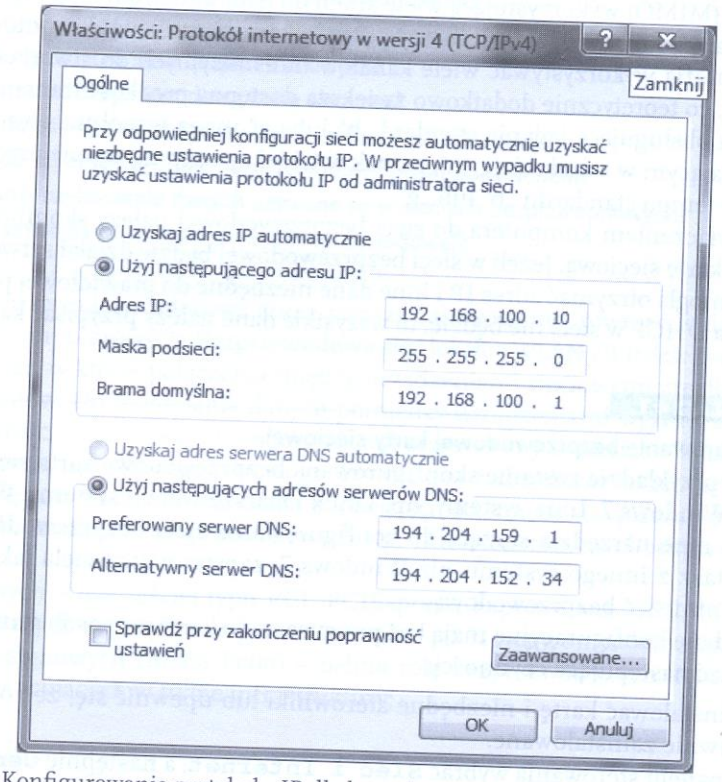
W tym przykładzie zostanie skonfigurowana bezprzewodowa karta sieciowa w systemie Windows 7. Inne systemy, np. Linux i starsze wersje systemu Windows, posiadają inne narzędzia służące do konfigurowania sieci bezprzewodowych. Jeżeli korzystasz z innego systemu niż Windows 7, zapytaj nauczyciela jak skonfigurować w nim sieć bezprzewodową.

Jeżeli dane konfiguracyjne mają być przypisane do karty w sposób statyczny, należy wykonać następujące czynności:

1. Zainstalować kartę i niezbędne sterowniki lub upewnić się, że zostały one poprawnie zainstalowane.
2. W panelu sterowania wybrać **Sieć i Internet**, a następnie **Centrum sieci i udostępniania**.
3. W oknie **Centrum sieci i udostępniania** wybrać polecenie **Zmień ustawienia karty sieciowej**.
4. W oknie **Połączenia sieciowe** kliknąć prawym klawiszem myszy ikonę symbolizującą konfigurowaną kartę i wybrać polecenie **Właściwości**.
5. Z rozwijanej listy wybrać **Protokół internetowy w wersji 4 (TCP/IPv4)** i kliknąć przycisk **Właściwości**.
6. W odpowiednie pola (rys. 4.1) wprowadzić dane konfiguracyjne:
   - adres IP,
   - maskę podsieci,
   - bramę domyślną,
   - adresy serwerów DNS (preferowanego i alternatywnego).

7. Kliknąć przycisk **OK**.
8. Upewnić się za pomocą polecenia `ipconfig /all`, że dane konfiguracyjne zostały wprowadzone poprawnie.

Sieć w trybie **ad hoc** charakteryzuje się zdecentralizowaną strukturą, w której przyłączone urządzenia mogą pełnić funkcje zarówno klientów, jak i punktów dostępowych. Do przekazywania danych nie jest wymagana żadna infrastruktura sieciowa, ponieważ pakiety dostarczane są bezpośrednio do odbiorcy. Sieci tego typu budowane są zazwyczaj na krótko i później demontuje się je. Wykorzystywane są np. do połączenia laptopa ze smartfonem lub tabletem. W Windows 7 w stworzeniu sieci ad hoc pomaga kreator, który prowadzi użytkownika przez cały proces konfiguracji.



Rys. 4.1. Konfigurowanie protokołu IP dla karty bezprzewodowej

PRZYKŁAD 4.2.

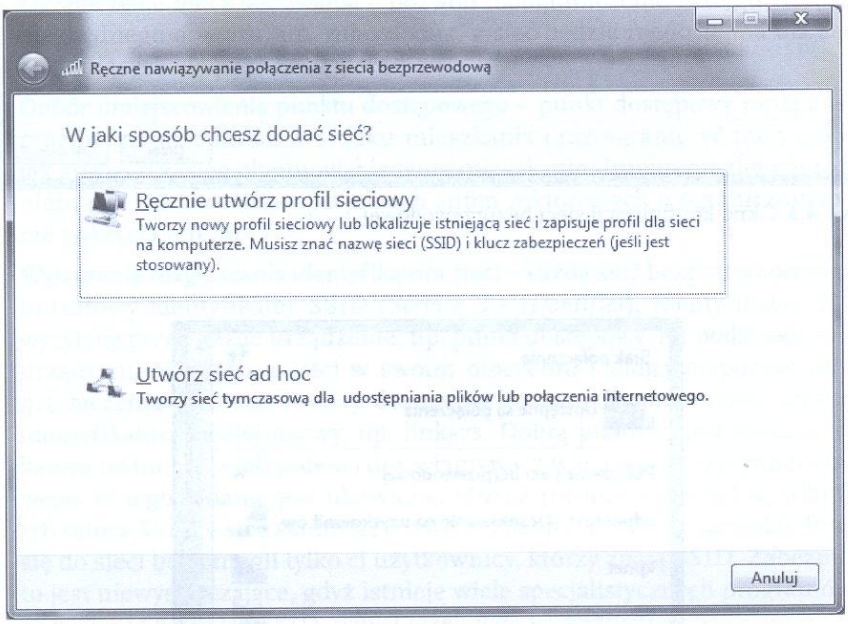
Konfigurowanie sieci ad hoc

W tym przykładzie zostanie skonfigurowana sieć ad-hoc w systemie Windows 7. Inne systemy, np. Linux i starsze wersje systemu Windows posiadają inne narzędzia służące do konfigurowania sieci bezprzewodowych. Jeżeli korzystasz z innego systemu niż Windows 7, zapytaj nauczyciela jak skonfigurować w nim sieć bezprzewodową.

Sieci ad hoc najczęściej budowane są jako rozwiązania tymczasowe, wykorzystywane do przesyłania plików pomiędzy dwoma urządzeniami. Ze względu na

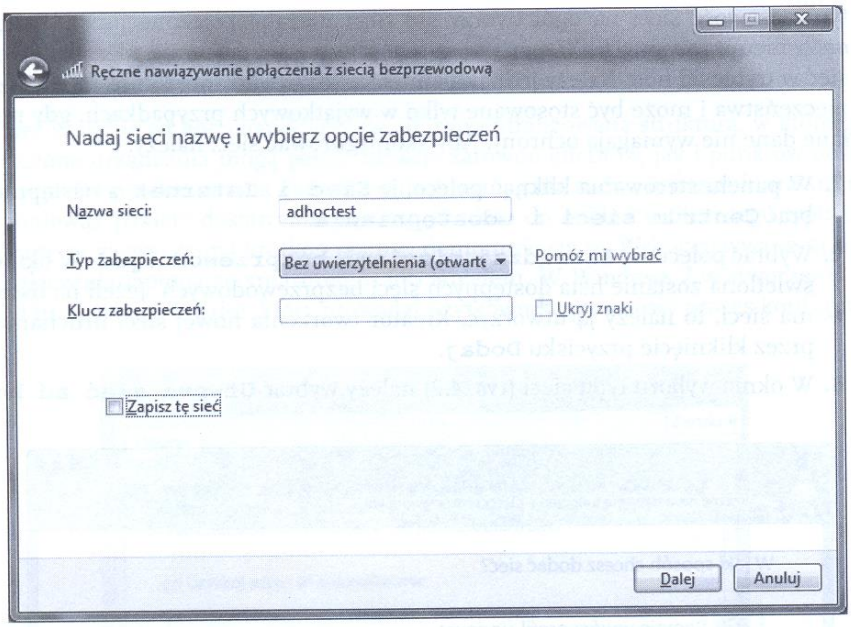
tymczasowość sieci na ogół tworzy się sieci niezabezpieczone przed dostępem osób nieuprawnionych. W tym ćwiczeniu zbudowana zostanie niezabezpieczona sieć w trybie ad hoc. Należy jednak pamiętać, że rozwiązanie to nie zapewnia bezpieczeństwa i może być stosowane tylko w wyjątkowych przypadkach, gdy przesyłane dane nie wymagają ochrony. Aby skonfigurować sieć, należy:

1. W panelu sterowania kliknąć polecenie **Sieć i Internet**, a następnie wybrać **Centrum sieci i udostępniania**.
2. Wybrać polecenie **Zarządzaj sieciami bezprzewodowymi**. W oknie wyświetlona zostanie lista dostępnych sieci bezprzewodowych. Jeżeli na liście nie ma sieci, to należy ją utworzyć. Kreator tworzenia nowej sieci uruchamia się przez kliknięcie przycisku **Dodaj**.
3. W oknie wyboru typu sieci (rys. 4.2) należy wybrać **Utwórz sieć ad hoc**.

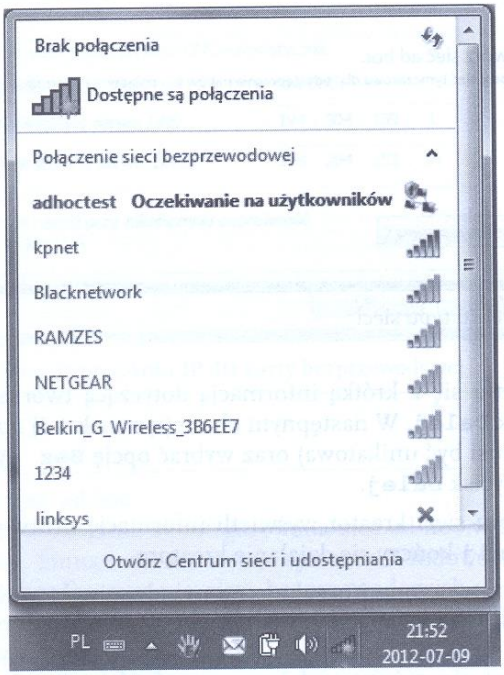


Rys. 4.2. Okno wyboru typu sieci

4. Po zapoznaniu się z krótką informacją dotyczącą tworzenia sieci należy wybrać przycisk **Dalej**. W następnym oknie (rysunek 4.3) należy wprowadzić nazwę sieci (musi być unikatowa) oraz wybrać opcję **Bez uwierzytelniania** i kliknąć przycisk **Dalej**.
5. Po utworzeniu sieci kreator wyświetli informację o utworzonej sieci. Przyciskiem **Zamknij** kończy się działanie kreatora.
6. Sieć jest już utworzona i oczekuje na urządzenia, które będą przyłączane do sieci (rys. 4.4).



Rys. 4.3. Okno konfiguracji sieci bezprzewodowej



Rys. 4.4. Okno dostępnych sieci bezprzewodowych

Sieci bezprzewodowe są narażone na podsłuch danych w znacznie większym stopniu niż sieci kablowe. Wynika to z faktu, że fale elektromagnetyczne rozchodzą się w całej przestrzeni, a każdy, kto znajdzie się w zasięgu rozprzestrzeniania się fal, może je odbierać (pod warunkiem, że posiada odpowiednie urządzenia). Aby zabezpieczyć sieć przed dostępem osób nieuprawnionych, należy zastosować następujące procedury:

1. **Zmiana domyślnego loginu i hasła punktu dostępowego** – wszystkie inne zabezpieczenia będą nieskuteczne, jeśli każdy będzie mógł zalogować się na naszym routerze i przejąć nad nim kontrolę. Listę domyślnych haseł routerów można znaleźć w internecie.
2. **Umożliwienie zarządzania tylko przez kabel** – wyłączenie możliwości logowania się do punktu dostępowego przez sieć bezprzewodową ogranicza dostęp do zarządzania urządzeniem tylko dla użytkowników podłączonych kablem.
3. **Ograniczenie mocy nadawania** – pozwoli na ograniczenie zasięgu sieci tylko do niezbędnego obszaru, np. mieszkania, a sieć będzie niedostępna dla sąsiadów znajdujących się poza zasięgiem.
4. **Dobór umiejscowienia punktu dostępowego** – punkt dostępowy można w miarę możliwości instalować w środku mieszkania oraz ograniczyć moc nadawania, tak aby jego zasięg obejmował jedynie mieszkanie. Innym możliwym rozwiązaniem jest zastosowanie specjalnych anten sektorowych o ograniczonym obszarze pokrycia terenu.
5. **Wyłączenie rozgłaszania identyfikatora sieci** – każda sieć bezprzewodowa posiada unikatowy identyfikator SSID (*Service Set IDentifier*). Identyfikator SSID jest wysyłany przez każde urządzenie, np. punkt dostępowy. Na podstawie tej nazwy urządzenia wykrywają sieci w swoim otoczeniu i mogą rozpocząć procedurę przyłączenia do sieci. Punkty dostępowe i routery standardowo używają jako identyfikatora swojej nazwy, np. linksys. Dobrą praktyką jest zmiana identyfikatora na inną – jeżeli potencjalny włamywacz wie, jaki jest typ punktu dostępowego, to jego zadanie jest ułatwione. Można również wyłączyć wysyłanie identyfikatora SSID – sieć stanie się niewidoczna dla typowych narzędzi. Przyłączyć się do sieci będą mogli tylko ci użytkownicy, którzy znają SSID. Zabezpieczenie to jest niewystarczające, gdyż istnieje wiele specjalistycznych programów, które są w stanie odczytać SSID, nawet jeżeli jego wysyłanie jest wyłączone.
6. **Włączenie filtrowania adresów MAC** – każda karta bezprzewodowa posiada unikatowy adres fizyczny MAC. Na jego podstawie punkt dostępowy może rozpoznać, czy jest to legalny użytkownik sieci czy intruz. Punkt dostępowy może mieć zdefiniowaną listę adresów MAC urządzeń, które powinny uzyskać dostęp do sieci (biała lista) i urządzeń, którym należy zabronić dostępu (czarna lista). Niestety, metoda filtrowania adresów MAC w obecnych czasach nie spełnia swojego zadania, ponieważ bardzo łatwo obejść to zabezpieczenie przez podmianę adresu MAC przez włamywacza. Mimo wszystko warto ją stosować.
7. **Włączenie szyfrowania danych** – brak szyfrowania sprawia, że nasze dane (loginy, hasła, numery kart) są przesyłane w sieci w sposób umożliwiający ich łatwe przechwycenie przez osoby trzecie.

Spośród wymienionych wyżej metod zwiększenia bezpieczeństwa sieci bezprzewodowych największe znaczenie praktyczne ma szyfrowanie danych. Obecnie w sieciach bezprzewodowych można spotkać trzy standardy zabezpieczenia danych:

- **WEP** (*Wired Equivalent Privacy*) – do ochrony danych w standardzie WEP wykorzystuje się algorytm RC4, który jest symetrycznym szyfrem strumieniowym z kluczem poufnym. Podczas szyfrowania metodą RC4 zostaje wykonana operacja różnicy symetrycznej XOR na bitach klucza i danych, której efektem jest szyfrogram. W celu odkodowania wiadomości odbiorca musi użyć tego samego klucza, który został użyty do zaszyfrowania wiadomości. W WEP stosowane są klucze o długości 64 lub 128 bitów (klucz składa się z 40 lub 104 bitów klucza i z tzw. wektora inicjalizującego o długości 24 bitów). W standardzie WEP oferowane są klucze poufne o długości 40 bitów, ponieważ w momencie opracowywania standardu prawo Stanów Zjednoczonych nie pozwalało na wykorzystywanie klucza dłuższego niż 40 bitów. Obecnie metoda WEP jest uznawana za niewystarczającą i powinna być stosowana tylko w przypadku, gdy urządzenia nie obsługują standardu WPA.
- **WPA** (*WiFi Protected Access*) – wykorzystuje protokoły TKIP (*Temporal Key Integrity Protocol*) oraz uwierzytelnienie EAP (*Extensible Authentication Protocol*). Został wprowadzony jako standard przejściowy pomiędzy WEP a WPA2. Zwiększenie bezpieczeństwa użytkowników sprzętu następuje bez konieczności wymiany sprzętu – wystarczy zmienić sterownik w karcie sieciowej lub firmware w punktach dostępowych. WPA może korzystać z trybu:
  - **Enterprise** – używa serwera RADIUS, który przydziela klucze odpowiednim użytkownikom.
  - **Personal** – wszystkie podłączone stacje wykorzystują jeden klucz dzielony przypisywany ręcznie przez administratora (PSK – *Pre-Shared Key*).
- **WPA2** (*WiFi Protected Access*) – zawiera poprawki eliminujące wszystkie znalezione luki w zabezpieczeniach WEP i WPA. W porównaniu z WPA wykorzystuje dynamiczne klucze o długości 128 bitów i automatycznie je dystrybuuje. Wykorzystuje algorytm szyfrowania AES. Jest zalecany do stosowania w sieciach bezprzewodowych.

Konfiguracja sieci bezprzewodowej pracującej w trybie infrastruktury składa się z dwóch kroków: konfiguracji punktu dostępowego i konfiguracji klienta sieci.

PRZYKŁAD 4.3.

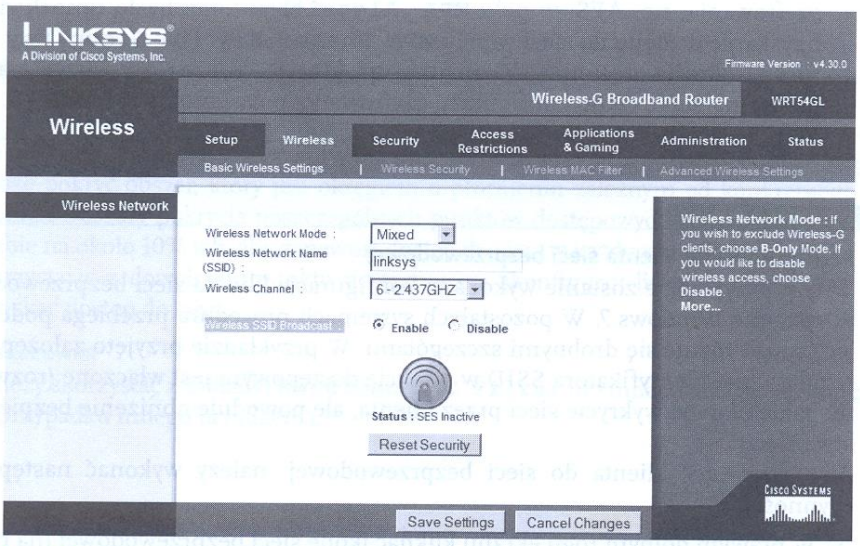
Konfigurowanie punktu dostępowego w routerze

W tym ćwiczeniu zostanie skonfigurowana bezprzewodowa sieć z włączonymi zabezpieczeniami. Konfiguracja zostanie pokazana na przykładzie routera z wbudowanym punktem dostępowym. Przed przystąpieniem do konfiguracji należy sprawdzić, jakie sieci bezprzewodowe działają na danym obszarze i jakie kanały są wykorzystywane. Aby kanały nie zakłócały się wzajemnie (w standardzie B i G zakresy częstotliwości kanałów częściowo zachodzą na siebie), odległości między wykorzystywanymi kanałami powinny być większe niż 6. Aby skonfigurować punkt dostępowy, należy wykonać następujące czynności:

1. Połączyć kablem kartę sieciową komputera z interfejsem sieciowym punktu dostępowego lub interfejsem LAN w przypadku routera z wbudowanym punktem dostępowym.

2. Skonfigurować kartę sieciową komputera i interfejs punktu dostępowego/routera do pracy w tej samej sieci (informacje o standardowej konfiguracji punktu dostępowego/routera można znaleźć w dokumentacji). Jeżeli hasło konta administratora nie jest znane, to można przywrócić urządzenie do stanu fabrycznego – w tym celu należy nacisnąć i przytrzymać przez 30 sekund przycisk **Reset**. Operacja ta usunie wszystkie ustawienia konfiguracyjne wprowadzone przez użytkownika.
3. W oknie wyszukiwarki wpisać adres urządzenia, np. 192.168.1.1, a w wyskakującym okienku wpisać nazwę konta administratora i hasło.
4. W zakładce **Wireless** wybrać **Basic Wireless Settings**, a następnie z listy rozwijanej wybrać tryb pracy (*Wireless Network Mode*). Dostępne tryby pracy to: tylko B (*B-only*), tylko G (*G-only*), mieszany, wykorzystujący jednocześnie B i G (*Mixed*), oraz wyłączony (*Disabled*). W pozostałych polach należy wpisać: identyfikator SSID w polu **Wireless Network Name**, numer kanału w polu **Wireless Channel**.
5. Za pomocą przycisku radiowego **Wireless SSID Broadcast** można włączyć (*Enable*) lub wyłączyć (*Disable*) rozgłaszanie identyfikatora SSID.
6. Kliknąć przycisk **Save Settings**.

Na rysunku 4.5 pokazano sposób konfiguracji punktu dostępowego.



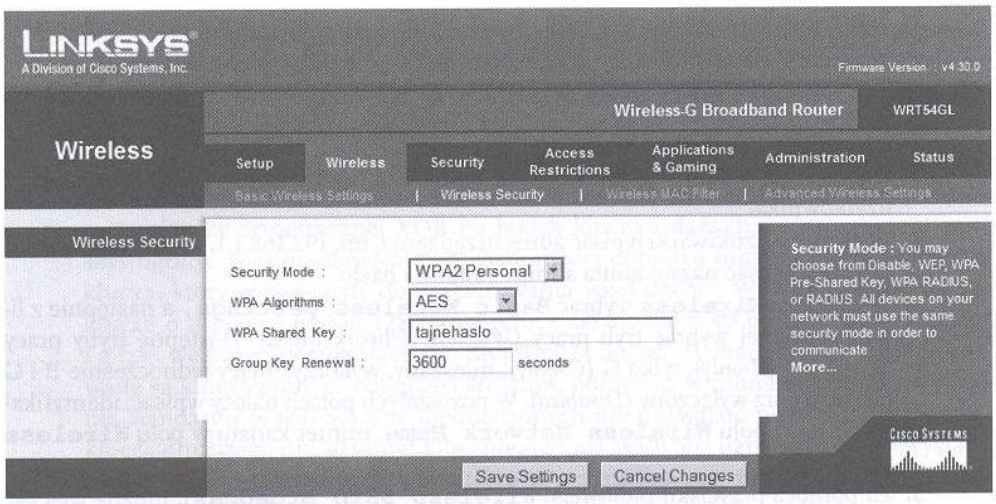
Rys. 4.5. Okno konfiguracji sieci bezprzewodowej w punkcie dostępowym

PRZYKŁAD 4.4.

Konfigurowanie szyfrowania sieci bezprzewodowej

Aby włączyć szyfrowanie danych przesyłanych w sieci bezprzewodowej, należy wykonać następujące czynności:

1. Połączyć kablem kartę sieciową komputera z interfejsem sieciowym urządzenia, a następnie za pomocą wyszukiwarki zalogować się na konto administratora.
2. W zakładce **Wireless** wybrać **Wireless Security**, a następnie z listy rozwijanej wybrać tryb szyfrowania, np. **WPA2 Personal**.



Rys. 4.6. Okno konfiguracji szyfrowania sieci bezprzewodowej

3. W polach okna konfiguracji należy wprowadzić: nazwę wybranego algorytmu szyfrowania, np. AES, w polu **WPA Algorithms** oraz hasło umożliwiające uzyskanie dostępu do sieci w polu **WPA Shared Key**. Pole **Group Key Renewal** określa częstotliwość zmian grupy kluczy – można pozostawić wartość domyślną 3600. Okno konfiguracji szyfrowania pokazano na rysunku 4.6.
4. Kliknąć przycisk **Save Settings**.

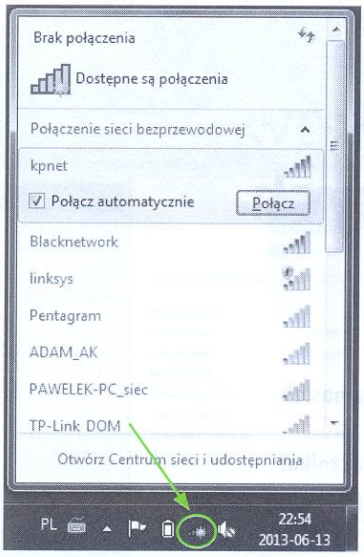
PRZYKŁAD 4.5.

Konfigurowanie klienta sieci bezprzewodowej

W tym przykładzie zostanie wykonana konfiguracja klienta sieci bezprzewodowej w systemie Windows 7. W pozostałych systemach procedura przebiega podobnie, lecz może różnić się drobnymi szczegółami. W przykładzie przyjęto założenie, że rozgłaszanie identyfikatora SSID w punkcie dostępowym jest włączone (rozwiązanie takie ułatwia wykrycie sieci przez klienta, ale powoduje obniżenie bezpieczeństwa sieci).

Aby przyłączyć klienta do sieci bezprzewodowej, należy wykonać następujące czynności:

1. W prawym dolnym rogu ekranu kliknąć ikonę sieci bezprzewodowej (na rysunku 4.7 zaznaczona strzałką).
2. W oknie dostępnych połączeń kliknąć wybraną sieć, zaznaczyć opcję **Połącz automatycznie**, a następnie kliknąć przycisk **Połącz**.
3. W oknie wprowadzić hasło dostępu do sieci zdefiniowane podczas konfiguracji punktu dostępowego.
4. Rozwinąć ponownie okno **Dostępne połączenia**, aby sprawdzić, czy istnieje połączenie z siecią (rysunek 4.8).



Rys. 4.7. Otwieranie okna dostępnych sieci bezprzewodowych

Rys. 4.8. Weryfikacja dostępnych sieci bezprzewodowych

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Zaplanuj rozmieszczenie minimalnej liczby punktów dostępowych tak, aby zapewnić pełne pokrycie obszaru Twojej szkoły. Dla uproszczenia przyjmij, że każdy punkt dostępowy może pokryć obszar, który jest okręgiem o promieniu zależnym od konkretnego urządzenia. Obszary pokrycia poszczególnych punktów dostępowych powinny zachodzić na siebie na około 10% tak, aby zapewnić dostęp do sieci w każdym punkcie szkoły.
2. Korzystając z dowolnego punktu dostępowego, skonfiguruj listę adresów, które mogą uzyskać dostęp do sieci.

Wskazówka

Należy skorzystać z zakładki **`Wireless MAC Filter`** lub innej o podobnym znaczeniu w przypadku innego urządzenia.