Bezprzewodowe Punkty Dostępowe

Standard / Pro / Advanced / Advanced+

Instrukcja użytkownika
język polski

Wersja: 2.9

Wersja polska: Atel Electronics. Opole, Sierpień 2003

Oświadczenie Federalnej Komisji Komunikacji (FCC - Federal Communication Commission) dotyczące zakłóceń

Sprzęt został przetestowany i spełnia ograniczenia sprzętu cyfrowego Klasy B, stosownie do Ustępu 15 przepisów FCC. Ograniczenia te zostały wprowadzone w celu właściwej ochrony przed szkodliwym wpływem zakłóceń na inne instalacje w budynku. Urządzenie wytwarza, używa i może wypromieniowywać energię na częstotliwościach radiowych i jeśli nie jest zainstalowane i używane zgodnie z zaleceniami, może powodować zakłócenia w komunikacji radiowej. Jakkolwiek nie ma gwarancji, że w specyficznych instalacjach zakłócenia nie będą się zdarzać. Jeśli to urządzenie jest przyczyną zakłóceń w odbiorze radiowym lub telewizyjnym, które może być spowodowane włączaniem i wyłączaniem urządzenia, użytkownik może spróbować zmienić wpływ urządzenia jednym z następujących sposobów:

- Zmienić kierunek lub umiejscowienie anteny odbiorczej.
- Zwiększyć odległość pomiędzy urządzeniem a odbiornikiem.
- Podłączyć urządzenie do innej sieci (gniazda) zasilania niż jest podłączony odbiornik.
- Skonsultować się ze sprzedawcą lub doświadczonym technikiem radiowo-telewizyjnym.

Ostrzeżenia FCC: Należy zapewnić bezpieczne warunki pracy urządzenia (np. używać tylko ekranowanego okablowania do podłączenia z komputerem lub urządzeń peryferyjnych). Jakiekolwiek zmiany lub modyfikacje niezatwierdzone przez komitet FCC mogą spowodować utratę prawa do posługiwania się przedstawionym w instrukcji urządzeniem.

Nadajnik nie może być zamieniony lub też pracować z jakąkolwiek inną anteną lub nadajnikiem.

Oświadczenie FCC dotyczące promieniowania: To urządzenie spełnia normy promieniowania określone przez FCC dla dowolnego środowiska. Urządzenie powinno być zainstalowane i zarządzane min. 20 cm od ciała użytkownika.

Urządzenie spełnia normy opisane w Ustępie 15 zarządzeń FCC. Działanie urządzenia jest przedmiotem dwóch następujących warunków:

1. Urządzenie nie powinno powodować szkodliwych zakłóceń,
2. Powinno być odporne na każde zakłócenie zewnętrzne, włącznie z zakłóceniami mogącymi spowodować nieprawidłowe działanie.

Oświadczenie zgodności z R&TTE

To urządzenie spełnia wszystkie wymagania Dyrektywy 1999/5/CE Parlamentu i Zgromadzenia Europejskiego z dnia 9.03.1999 o sprzęcie radiowym i terminalach telekomunikacyjnych oraz wzajemnym rozpoznawaniu i zgodności. (R&TTE).

Dyrektywa R&TTE odwołała i zastąpiła zarządzenia 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) 8.04.2000.

Bezpieczeństwo

Urządzenie zostało zaprojektowane z najwyższą troską o bezpieczeństwo instalatora i użytkownika. Jakkolwiek powinno się zwrócić specjalną uwagę na niebezpieczeństwo porażenia elektrycznego lub elektrostatycznego podczas pracy ze sprzętem elektrycznym. Przestrzeganie wszystkich tych wskazówek oraz producentów komputerowych zapewni bezpieczne użytkowanie sprzętu.

Sprzęt został dopuszczony do użytku w Polsce

1. Urząd Regulacji Telekomunikacji i Poczty stwierdza, że Urządzenie IWE-1100 pracujące:
   - w zakresie częstotliwości 2,400 – 2,4835 GHz
   - z sekwencyjnym rozpraszaniem widma (DSSS)

   spełniają wymagania zasadnicze określone w ustawie z dnia 21 lipca 2000r. – Prawo Telekomunikacyjne (Dz. U. z 2000r. Nr 73, poz. 852). Potwierdzenie zgodności posiada numer CLBT/C/356/2002
2. Urządzenia zostały dopuszczone do użytku w Polsce w zestawieniu:
   - radiowy punkt dostępowy - IWE1100
   - antenna – Patria 10/2.4GHz, Partner 15/2.4GHz, Radius XP 17/2.4GHz, Vector 19/2.4GHz,
   - kabel antenowy – H155 ze złączami RSMA / N,

   na podstawie deklaracji zgodności wydanej przez URTiP CLBT/C/187/2003.
   Zestawy posiadają potwierdzenie zgodności w następującej konfiguracji:
   - IWE1100, antena Patria 10dBi, kabel H155 ≥ 10mb
   - IWE1100, antena Partner 15dBi, kabel H155 ≥ 21mb
   - IWE1100, antena Radius XP 17dBi, kabel H155 ≥ 25mb
   - IWE1100, antena Vector 19dBi, kabel H155 ≥ 30m

1 Wprowadzenie

1.1 Przegląd

Bezprzewodowy punkt dostępowy (access point - AP) pracujący w standardzie IEEE 802.11.b umożliwia bezprzewodowe połączenie stacji roboczych do zasobów sieci LAN zgodnie ze standardem Ethernet. Dostępne są cztery różne modele: Standard, Pro, Advanced oraz Advanced+, których podział wynika z posiadanych cech. Wersja Standard posiada najmniejsze możliwości, wersja Advanced+ największe. Urządzenia niezależnie od wersji wyposażone są w interfejs zarządzania poprzez strony WWW oraz program Wireless Network Manager.
W rozdziale 2. opisane są kolejne kroki instalacji i konfiguracji nowego punktu dostępowego, co pozwala na szybkie przygotowanie urządzenia do pracy. W rozdziale 3 zawarte jest szczegółowe objaśnienie każdej ze stron WWW służącej do zarządzania. Pozwoli to użytkownikowi zrozumieć, jak dobrać ustawienia punktu dostępowego według własnych potrzeb. Dodatkowo opisano konfigurację urządzenia poprzez strony WWW oraz konfigurację i monitoring punktów dostępowych w programie Wireless Network Manager. W celu uzyskania więcej informacji o programie należy sięgnąć do pomocy w Internecie.

1.2 Cechy charakterystyczne

- **Resetowanie ustawień.** Przywracanie ustawień fabrycznych urządzenia.
- **IEEE 802.11b**
  - **Access Point.** Przesyłanie pakietów pomiędzy bezprzewodowym interfejsem sieci IEEE 802.11b (klienci bezprzewodowi) a przewodową siecią Ethernet LAN.
  - **64 i 128 bitowy WEP (Wired Equivalent Privacy**). Autoryzacja i szyfrowanie danych.
  - **Włączanie/wyłączanie rozgłaszania SSID**. Administrator może włączyć lub wyłączyć rozgłaszanie SSID ze względów bezpieczeństwa. Gdy funkcja rozgłaszania SSID jest wyłączona, komputer-klient nie może połączyć się z punktem dostępowym podając dowolną nazwę sieci (SSID, Service Set ID); prawidłowe SSID powinno być wtedy podane na kliencie.
  - **Kontrola dostępu na podstawie adresu MAC**. Blokowanie nieautoryzowanych klientów bezprzewodowych na podstawie adresów MAC (Media Access Control).
  - IEEE 802.1x/RADIUS. Rozpoznawanie użytkownika i dynamiczna dystrybucja kluczy szyfrujących prowadzona przez protokół IEEE 802.1x Port Based Network Access Control lub RADIUS (Remote Authentication Dial-In User Service).
  - **Izolacja klienta bezprzewodowego**. Ruch pomiędzy dwoma sieciami bezprzewodowymi może być blokowany tak, by poszczególne stacje nie widziały się wzajemnie. Ta właściwość może być wykorzystana w publicznych punktach dostępowych (tzw. hotspotach) do zabezpieczenia użytkowników przed atakami hakerów.
  - **Repeater**. Punkt dostępowy może komunikować się z innymi punktami dostępowymi lub mostami bezprzewodowymi poprzez WDS (Wireless Distribution System - Bezprzewodowy System Dystrybucji). Punkt dostępowy może przesyłać pakiety od bezprzewodowych klientów do innych punktów dostępowych, a te z kolei do sieci Ethernet.
  - **Równoważenie obciążenia punktu dostępowego**. Niektóre punkty dostępowe mogą tworzyć grupy równoważenia obciążenia. W ramach takiej grupy dołączanie użytkowników bezprzewodowych oraz ruch przez nich generowany może być przenoszony między poszczególne punkty dostępowe.
  - **Kontrola zasilania nadajnika**. Moc nadawania modułu radiowego (RF - Radio Frequency) może być dopasowywana do zmiany obszaru pokrycia punktu dostępowego.
  - **Wymienna antena**. Anteny montowane fabrycznie mogą być w różnych celach zastąpione przez anteny zewnętrzne o większej mocy.
  - **Wykaz podłączonych klientów**. Wykaz statusów wszystkich bezprzewodowych klientów podłączonych do punktu dostępowego.
- **Klient DHCP.** Punkt dostępowy może automatycznie otrzymać adres IP z serwera DHCP.
- **Serwer DHCP**. Punkt dostępowy może automatycznie przydzielać adresy IP komputerom lub innym urządzeniom dzięki protokołowi DHCP.
  - **Statyczne DHCP**. Administrator może na stałe przydzielić adres IP do danego adresu MAC tak, że zawsze określony adres IP będzie się odnosił do urządzenia o określonym adresie MAC.
  - **Wykaz aktualnych powiązań DHCP**. Funkcja ta pokazuje, jakie adresy IP są przydzielone do hostów identyfikowanych poprzez adresy MAC. Narzędzia do zmiany oprogramowania (firmware'u)
  - **Aktualizacja firmware'u**. Oprogramowanie punktu dostępowego może być aktualizowane, w celu dodawania nowych funkcji w przyszłości.
    - Xmodem-based. Aktualizacja oprogramowania poprzez port szeregowy RS232.
    - TFTP-based. Aktualizacja oprogramowania przez TFTP (Trivial File Transfer Protocol).

- **Kopia zapasowa ustawień.** Ustawienia konfiguracyjne punktu dostępowego mogą być archiwizowane do pliku poprzez TFTP w celu późniejszego ich przywrócenia.

- **Zarządzanie**
  - *Program Wireless Network Manager* do konfigurowania, monitorowania i diagnozowania komputera lokalnego i sąsiadujących punktów dostępowych. Protokół zarządzania oparty jest na adresach MAC.
  - *Network Manager oparty na WWW* do konfigurowania i monitorowania punktów dostępowych.Protokół zarządzania oparty jest na HTTP (HyperText Transfer Protocol). Pozwala na zarządzanie przez przeglądarkę internetową.
  - *SNMP*. Wsparcie dla SNMP (Simple Network Management Protocol) MIB I, MIB II, IEEE 802.1d, IEEE 802.1x oraz Private Enterprise MIB.
  - *UPnP* (Universal Plug and Play). Punkt dostępowy odpowiada na komunikaty UPnP tak, że użytkownicy Windows XP mogą znaleźć punkt dostępowy na zakładce Moje Miejsca Sieciowe (My Network Places) i używać przeglądarki internetowej do jego zarządzania.
  - *Telnet*. Użytkownik ma możliwość zarządzania punktem dostępowym przez Telnet.
  - *Zasilanie z sieci Ethernet* (opcjonalnie). Dostarczanie zasilania dla punktu dostępowego przez okablowanie ethernetowe przy pomocy technologii PowerDsine (http://www.powerdsine.com) - (zgodne z przyszłą normą IEEE 802.3af). Ta cecha ułatwia budowanie rozległych bezprzewodowych sieci LAN.
  - *Sprzętowy nadzór* (watchdog). Automatyczne wykrywanie nieprawidłowej pracy urządzenia i jego restart.

1.3 Porównanie cech

	Standard	Pro	Advanced	Advanced+
Repeater (Wireless Distribution System)		+	+	+
Serwer DHCP		+	+	+
Telnet		+	+	+
IEEE 802.1x / RADIUS			+	+
SNMP IEEE 802.1x MIB			+	+
Izolacja klientów				+
Równoważenie obciążenia				+

2 Pierwsza instalacja i konfiguracja

2.1 Instalowanie dołączonej karty WLAN PCMCIA

Niektóre modele punktów dostępowych jako interfejsu sieciowego używają karty WLAN PCMCIA montowanej do gniazda PCMCIA nazwanego Wireless LAN Card. Jeśli punkt dostępowy i dołączona karta WLAN PCMCIA są zapakowane oddzielnie, po wyjęciu z pudełka należy włożyć kartę do odpowiedniego slotu PCMCIA. Następnie należy podłączyć zasilacz do gniazda w punkcie dostępowym i włączyć urządzenie.

UWAGA: Dopóki urządzenie jest zapakowane lub przenoszone na większe odległości nie należy wyciągać karty PCMCIA z gniazda.

2.2 Wybór źródła zasilania

Urządzenie może być zasilane z dołączonego zasilacza lub poprzez PoE (Power oper Ethernet) i automatycznie dostosowuje się do decyzji użytkownika.

Gdy źródłem energii ma być zasilacz:
1. Podłączyć zasilacz do sieci elektrycznej.
2. Włożyć wtyczkę zasilacza do odpowiedniego gniazda w urządzeniu.

UWAGA: Prąd wyjściowy o stałym napięciu (DC) 5V i natężeniu min. 1A.

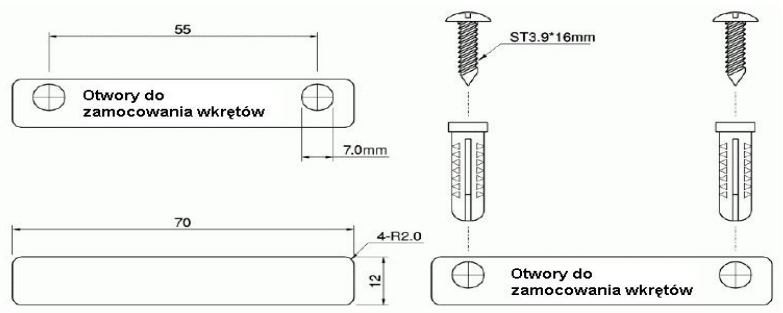
Zasilanie urządzenia przez PoE (z sieci Ethernet):
1. Podłączyć wtyczkę kabla ethernetowego (skrętki) do wolnego portu huba obsługującego PoE.
2. Podłączyć drugi koniec skrętki do portu LAN/CONFIG urządzenia.

UWAGA: Cecha PoE urządzenia jest zgodna z PowerDsine. Po więcej informacji zajrzyj na stronę internetową PowerDsine (http://www.powerdsine.com).

2.3 Montowanie urządzenia na ścianie

Jeśli jest to konieczne, urządzenia może być zamontowane na ścianie.

1. Przykleić dołączoną naklejkę na ścianę.
2. W miejscach krzyżyków wywiercić dziurę o średnicy 7mm i głębokości 25mm.
3. Do każdej z dziur włożyć dołączony do zestawu plastikowy kołek.
4. Do każdego kołka wkręcić na odpowiednią głębokość dołączony do zestawu wkręt.
5. Powiesić urządzenie na ścianie.



Rys. 1. Montaż urządzenia na ścianie.

2.4 Przygotowanie do konfiguracji

Aby skonfigurować punkt dostępowy, potrzebny jest komputer zarządzający z zainstalowaną przeglądarką internetową. Podczas pierwszej konfiguracji punktu dostępowego komputer zarządzający powinien mieć zainstalowaną kartę

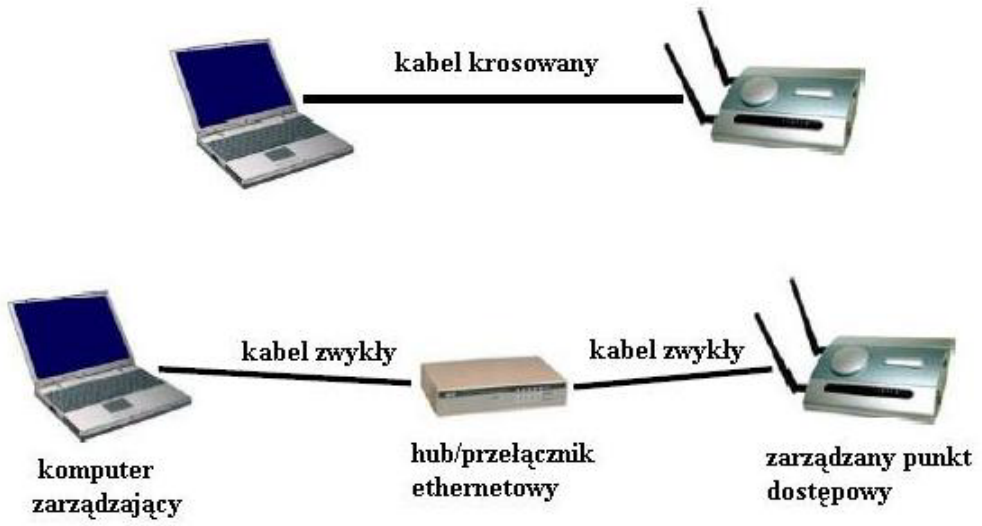
sieciową. Do późniejszego administrowania danym urządzeniem może być wykorzystany zarówno komputer bezprzewodowy, jak i podłączony kablem do sieci Ethernet.

> **UWAGA:** Jeśli pracuje się z przeglądarką Opera, aby konfigurować punkt dostępowy należy kliknąć menu File/Plik, kliknąć Preferences.../Ustawienia..., File types/Typy plików i zmienić typ MIME text/html, dodając rozszerzenie pliku ".sht" tak, aby Opera mogła pracować właściwie z internetowymi stronami zarządzania punktem dostępowym.

Gdy protokół konfiguracji/zarządzania bazuje na HTTP należy się upewnić czy adres IP komputera zarządzającego i adres IP zarządzanego urządzenia należą do tej samej podsieci (domyślny adres IP punktu dostępowego wynosi 192.168.0.1, a jego domyślna maska podsieci 255.255.255.0).

2.5 Połączenie komputera zarządzającego z punktem dostępowym

Do połączenia komputera zarządzającego z punktem dostępowym do pierwszej konfiguracji za pomocą skrętki można skorzystać z dwóch możliwości, zilustrowanych na Rys. 2.



Rys. 2. Połączenie komputera zarządzającego i punktu dostępowego.

Można użyć kabla krosowego (jedna taka skrętka znajduje się w zestawie) lub huba czy przełącznika i dwóch zwykłych kabli ethernetowych.

> **UWAGA:** W celu konfiguracji jedna wtyczka skrętki musi być podłączona do gniazda ethernetowego LAN/CONFIG punktu dostępowego.

2.5.1 Zmiana ustawień TCP/IP komputera zarządzającego

Należy zmienić ustawienia TCP/IP komputera zarządzającego tak, aby jego adres IP i adres IP punktu dostępowego należały do tej samej podsieci. Ustawić adres IP komputera na jeden z zakresu 192.168.0.xxx (domyślny adres IP urządzenia wynosi 192.168.0.1), a maskę sieciową na 255.255.255.0.

> **UWAGA:** Niektóre wersje systemu Windows muszą być restartowane, aby zmiany ustawień TCP/IP odniosły skutek.
>
> **WSKAZÓWKA:** Po połączeniu komputera zarządzającego z punktem dostępowym przez sieć Ethernet można zainstalować program Wireless Network Manager na tym komputerze i administrować punktem dostępowym bez konieczności ingerencji w ustawienia TCP/IP komputera zarządzającego. Po więcej informacji o programie należy zajrzeć do pomocy on-line.

2.6 Konfigurowanie punktu dostępowego

Po rozwiązaniu wszystkich kwestii związanych z adresacją IP należy uruchomić przeglądarkę internetową na komputerze zarządzającym. Następnie przejść pod adres "http://192.168.0.1" na stronę Web-based Network Manager.

UWAGA: Jeśli korzysta się z przeglądarki Opera (firmy Opera Software), aby konfigurować punkt dostępowy należy kliknąć menu File/Plik, kliknąć Preferences.../Ustawienia..., File types/Typy plików i zmienić typ MIME text/html, dodając rozszerzenie pliku ".sht" tak, aby Opera mogła pracować właściwie z internetowymi stronami zarządzania punktem dostępowym.

WSKAZÓWKA: Do późniejszej konfiguracji urządzenia przez przeglądarkę można użyć host name (nazwy hosta) punktu dostępowego. Np. jeśli punkt dostępowy nazywa się "AP", można wejść na jego stronę zarządzania (Web-based Network Manager) przez adres "http://AP".

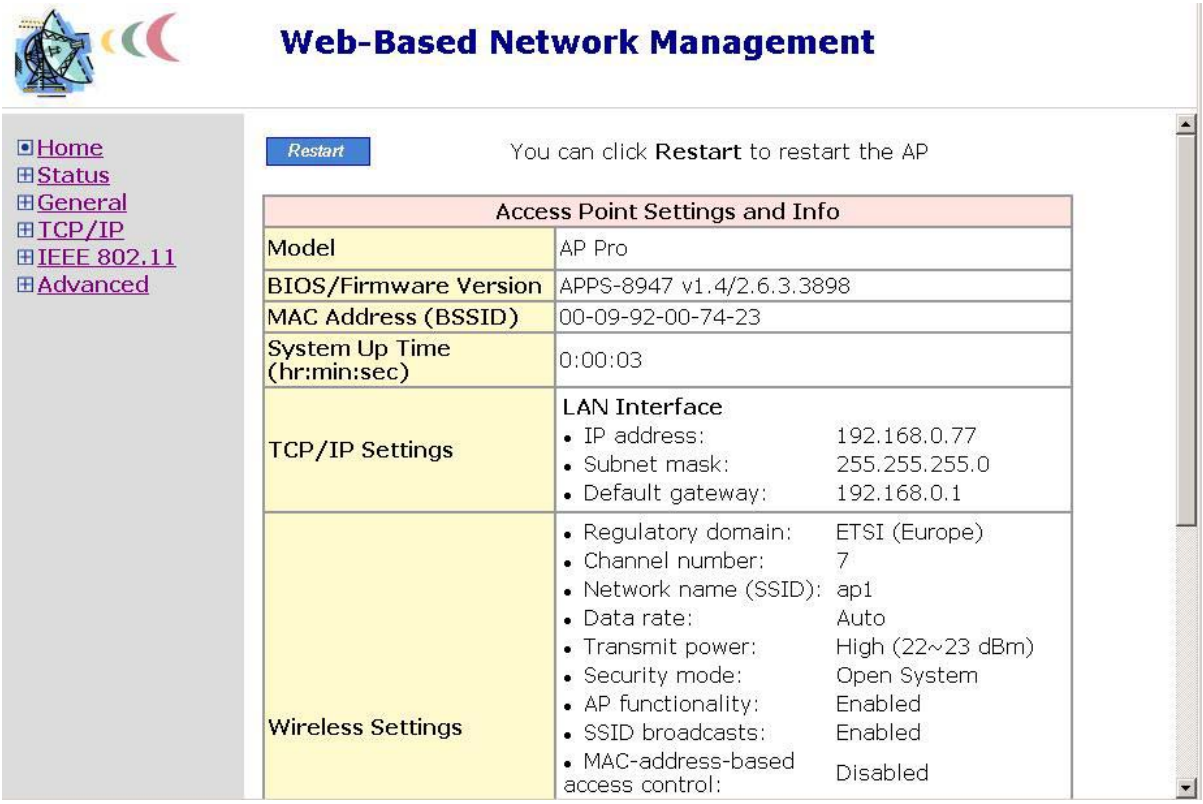
2.6.1 Wprowadzanie Nazwy użytkownika i Hasła

Zanim pojawi się strona startowa Web-based Network Manager, użytkownik jest proszony o podanie Nazwy użytkownika i Hasła. Podczas pierwszej konfiguracji należy użyć domyślnych ustawień: Nazwa użytkownika - "**root**" oraz Hasło - "**root**".

Rys. 3. Wprowadzanie nazwy użytkownika i hasła.

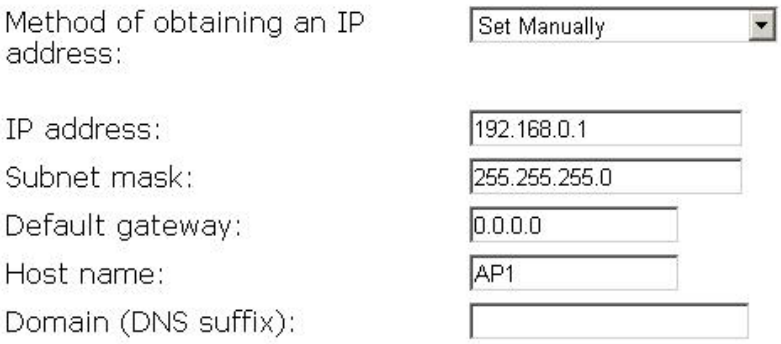
UWAGA: Zaleca się zmianę hasła domyślnego z powodów bezpieczeństwa. Hasło można zmienić klikając na link General, Password (więcej informacji znajdziesz w rozdziale 3.3.1).

WSKAZÓWKA: Gdy wyświetli się strona zawierająca aktualne ustawienia i status punktu dostępowego, można ją zapisać lub wydrukować z przeglądarki, by ewentualnie przejrzeć ją w przyszłości.



Rys. 4. Strona startowa.

2.6.2 Krok 1: Konfigurowanie ustawień TCP/IP

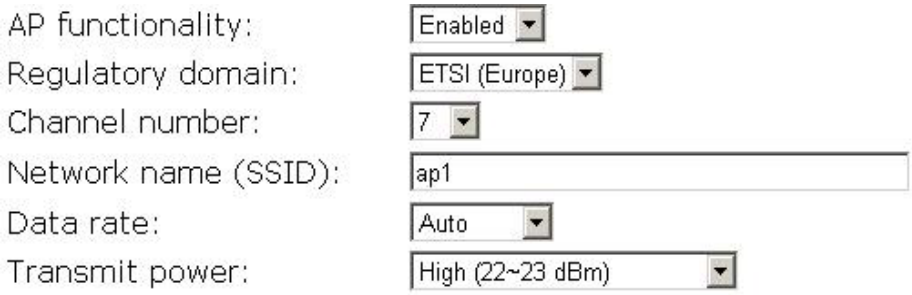


Rys. 5. Ustawienia TCP/IP.

Aby skonfigurować ustawienia adresacji IP należy przejść do sekcji TCP/IP, Addressing. Adres IP może być ustawiony ręcznie lub przydzielony automatycznie przez serwer DHCP z sieci LAN. Jeśli ręcznie ustawiany jest IP adress (adres IP), Subnet mask (maskę podsieci) i Default gateway (bramę domyślną), należy zrobić to właściwie, aby ustawienia były zgodne z otoczeniem sieci LAN. Dodatkowo można określić Host Name (nazwę hosta) i Domain (DNS suffix), czyli domenę punktu dostępowego.

Po zakończeniu należy kliknąć na przycisk Save (Zapisz), który znajduje się na dole strony. Nastąpi powrót do strony startowej.

2.6.3 Krok 2: Konfigurowanie ustawień IEEE 802.11



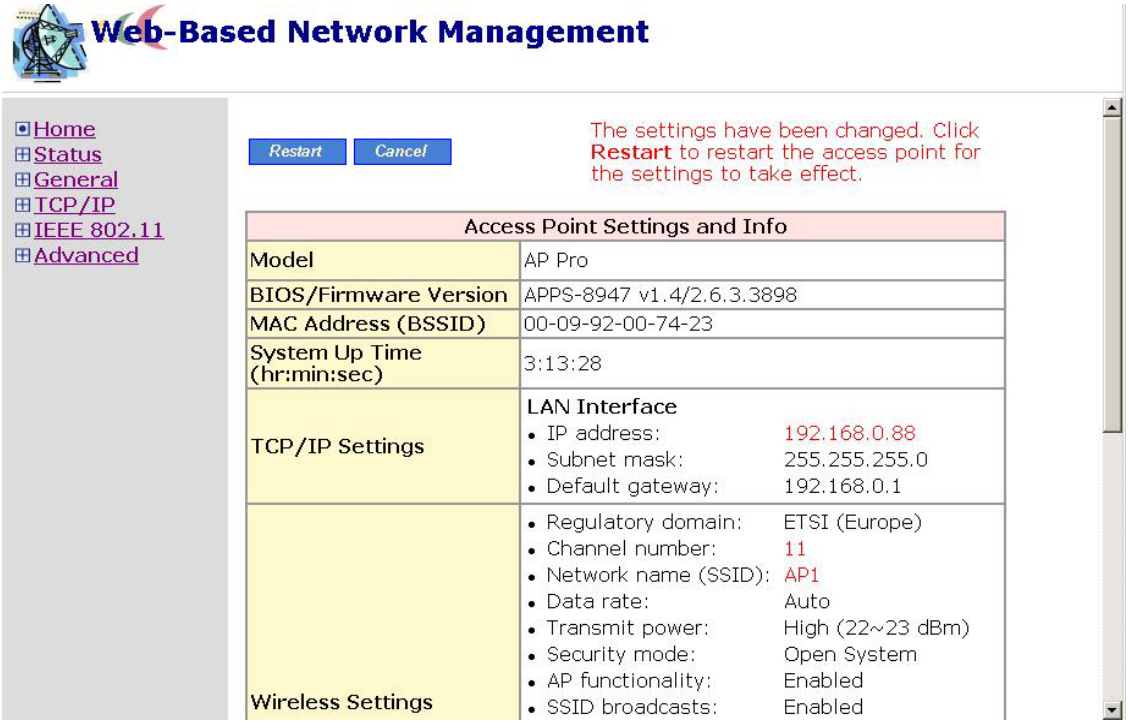
Rys. 6. Ustawienia komunikacji IEEE 802.11b.

W sekcji IEEE 802.11, Communication, można skonfigurować ustawienia komunikacji związanej ze standardem IEEE 802.11b; m.in. Regulatory domain (Regulacje prawne), Channel number (Numer kanału) i Network name (SSID) (Nazwa sieci).

Liczba dostępnych kanałów częstotliwości (RF) zależy od lokalnych uregulowań prawnych; dlatego powinno się wybrać odpowiednią opcję w Regulatory domain w zależności od regionu, w którym urządzenie będzie pracowało. Nazwa SSID klienta bezprzewodowego i punktu dostępowego powinna być identyczna, aby oba urządzenia mogły się komunikować.

Po zakończeniu trzeba kliknąć na przycisk Save (Zapisz), który znajduje się na dole strony. Nastąpi powrót do strony startowej.

2.6.4 Krok 3: Przeglądanie i zatwierdzanie ustawień



Rys. 7. Zmiany w ustawieniach są zaznaczone na czerwono.

Na stronie głównej można przejrzeć wszystkie zmiany ustawień, które zostały wprowadzone. Zmiany są podświetlone na czerwono. Jeśli są poprawne, należy kliknąć przycisk Restart, aby zrestartować urządzenie, nastąpi wprowadzenie nowych ustawień.

UWAGA: Proces restartu punktu dostępowego wynosi do 10s.

2.7 Rozmieszczanie punktu dostępowego

Po wykonanej konfiguracji punktu dostępowego, należy umieścić urządzenie w wyznaczonym miejscu i podłączyć do sieci LAN poprzez przełącznik (switch).

2.8 Ustawianie komputerów klienckich

Ustawienia TCP/IP wraz z ustawieniami IEEE 802.11b klientów bezprzewodowych muszą być dopasowane do ustawień punktu dostępowego.

2.8.1 Konfigurowanie ustawień powiązanych z IEEE 802.11b

Zanim bezprzewodowy komputer kliencki będzie mógł się komunikować z innymi hostami w sieci opartej na TCP/IP, trzeba utworzyć bezprzewodowe połączenie z punktem dostępowym.

Aby ustanowić bezprzewodowe połączenie z punktem dostępowym należy:

1. Uruchomić program konfiguracyjny/monitorujący dostarczony przez sprzedawcę karty sieciowej.
2. Użyć programu do odpowiedniego ustawienia opcji: Operating Mode, SSID oraz WEP (Wired Equivalent Privacy - metoda zabezpieczania transmisji).

UWAGA: Bezprzewodowy komputer-klient musi pracować w trybie infrastructure, aby mógł się połączyć z punktem dostępowym.

UWAGA: Nazwa SSID klienta musi być identyczna z SSID punktu dostępowego. Albo, w przypadku gdy właściwość SSID broadcasts (rozgłaszanie SSID) punktu dostępowego jest włączona (domyślnie), SSID klienta bezprzewodowego może być ustawiona na “any” (“jakikolwiek”).

UWAGA: Komputer-klient, jak i punkt dostępowy muszą mieć te same ustawienia WEP, aby mogły się wzajemnie komunikować.

UWAGA: Dla lepszego bezpieczeństwa sieci bezprzewodowych właściwość IEEE 802.1x punktu dostępowego powinna być włączona tak, by tylko autoryzowani klienci mogli się podłączyć do sieci. Więcej o zabezpieczaniu sieci WLAN metodą IEEE 802.1x znajduje się na dołączonej płycie CD.

2.8.2 Konfigurowanie ustawień powiązanych z TCP/IP

Aby dołączyć klientów bezprzewodowych (ze statycznym adresem IP) do Punktu Dostępowego należy zmienić ustawienia TCP/IP komputerów klienckich tak, aby ich adresy IP należały do tej samej podsieci, co adres punktu dostępowego. Jeśli w sieci znajduje się serwer DHCP należy włączyć opcję automatycznego przydzielania adresu IP.

UWAGA: Niektóre wersje systemu Windows wymagają restartu, aby zmiany ustawień TCP/IP odniosły skutek.

2.9 Zatwierdzanie ustawień punktu dostępowego i komputerów klienckich

Po zakończeniu ustawiania punktu dostępowego i konfigurowania klientów, należy sprawdzić, czy wprowadzone ustawienia, są prawidłowe.

2.9.1 Sprawdzanie czy ustawienia powiązane z IEEE 802.11b działają

Aby sprawdzić czy klient bezprzewodowy komunikuje się z punktem dostępowym należy:

1. Uruchomić program do konfiguracji/monitoring dostarczony przez sprzedawcę zainstalowanej karty sieciowej WLAN.
2. Sprawdzić czy komputer jest powiązany z punktem dostępowym i czy jest to właściwe urządzenie.

Jeśli sprawdzenie wypadnie niepomyślnie, należy zajrzeć do Załącznika B-1 “Problemy ustawień sieci bezprzewodowych” w celu rozwiązania problemów.

2.9.2 Sprawdzanie czy ustawienia powiązane z TCP/IP działają

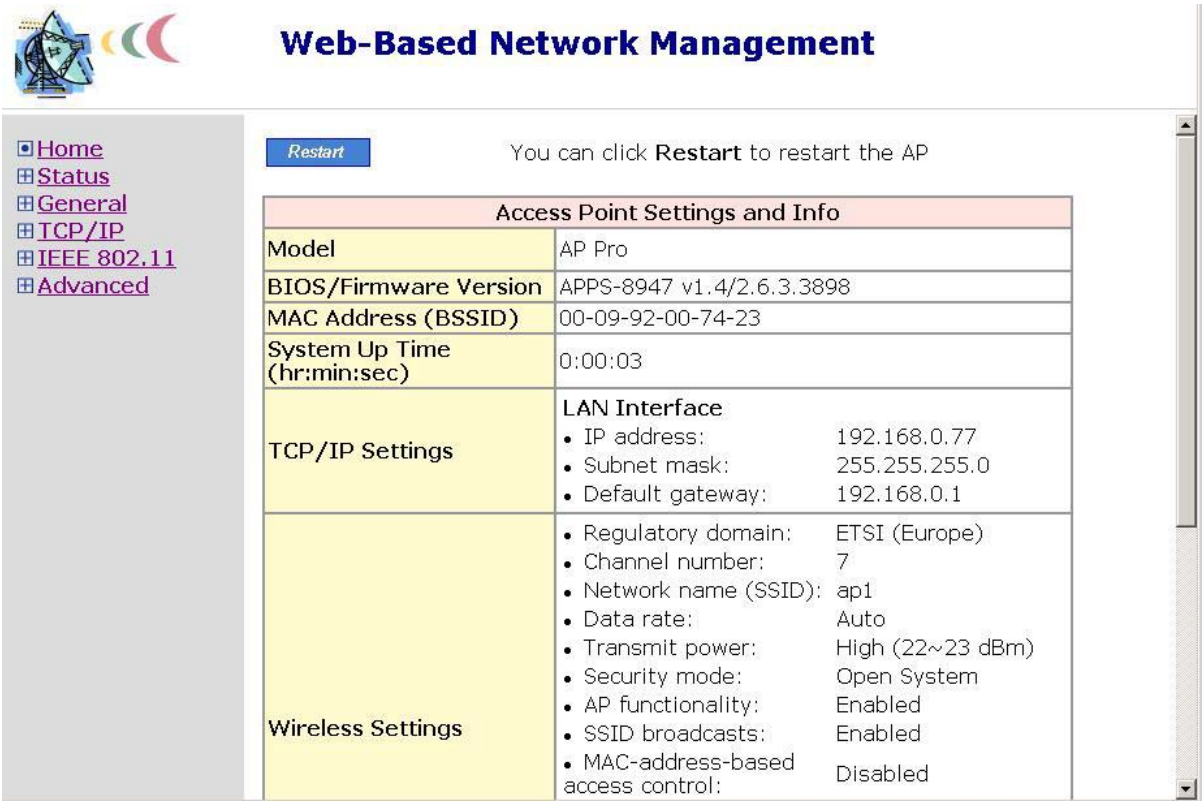
Aby sprawdzić czy komputer-klient ma dostęp do Internetu należy:

1. Uruchomić Tryb poleceń (Windows Command Prompt) na kliencie: Start, Run/Uruchom...
2. W otwartym oknie wpisać "ping adresIP", gdzie adresIP to adres IP urządzenia (punktu dostępowego). Podmienić tą nazwę rzeczywistym adresem IP, np. ping 192.168.0.1. Następnie wciśnąć Enter.
1. Jeśli punkt dostępowy odpowiada, przejść do następnego punktu. W przeciwnym wypadku zajrzeć do Załącznika B-2 "Problemy ustawień TCP/IP" w celu rozwiązania problemów.
2. Wpisać "ping brama_domyślna", gdzie brama_domyślna jest adresem IP bramy domyślnej klienta bezprzewodowego. Następnie wciśnąć Enter.
3. Jeśli bramka odpowiada, przejść do następnego punktu. W przeciwnym wypadku zajrzeć do Załącznika B-2 "Problemy ustawień TCP/IP" w celu rozwiązania problemów.
4. Wpisać "ping 1serwerDNS", gdzie 1serwerDNS jest adresem IP pierwszego serwera DNS komputera bezprzewodowego. Następnie wciśnąć Enter.
5. Jeśli ten serwer DNS odpowiada, przejść do następnego punktu. W przeciwnym wypadku zajrzeć do Załącznika B-2 "Problemy ustawień TCP/IP" w celu rozwiązania problemów.
6. Wpisać "ping 2serwerDNS", gdzie 2serwerDNS jest adresem IP drugiego serwera DNS komputera bezprzewodowego. Następnie wcisnąć Enter.
7. Jeśli ten serwer DNS odpowiada, nie powinno być już problemów sieciowych z TCP/IP. W przeciwnym wypadku zajrzęć do Załącznika B-2 "Problemy ustawień TCP/IP" w celu rozwiązania problemów.

3 Używanie menadżera sieciowego opartego na stronach WWW

W tym rozdziale zostanie wyjaśniona każda strona internetowa do zarządzania programem Web-based Network Manager.

3.1 Przegląd



Rys. 8. Strona startowa.

3.1.1 Struktura menu

Lewa część strony startowej zawiera menu, dzięki któremu można wydawać polecenia dla punktu dostępowego. Poniżej znajduje się krótki opis linków tego menu:

Home. Powrót do strony startowej (głównej).
Status. Przegląd informacji.
- *Wireless Clients*. Informacje o klientach bezprzewodowych aktualnie podłączonych do punktu dostępowego.
- *DHCP Mappings*. Aktualne zestawienie adresów IP i MAC wbudowanego serwera DHCP.

General. Opcje ogólne.
Password. Otrzymywanie prawa do zmiany ustawień punktu dostępowego.
- *Firmware Tools*. Do aktualizacji oprogramowania urządzenia oraz zapisywania i przywracania ustawień konfiguracyjnych punktu dostępowego.

TCP/IP. Ustawienia związane z TCP/IP.
- *Addressing*. Ustawienia adresacji IP punktu dostępowego, aby mógł pracować w sieci opartej na TCP/IP.
- *Serwer DHCP*. Ustawienia dla serwera DHCP (Dynamic Host Configuration Protocol) na punkcie dostępowym.

IEEE 802.11. Ustawienia związane z IEEE 802.11b.
- *Communication*. Podstawowe opcje interfejsu IEEE 802.11b punktu dostępowego pracującego aktualnie z klientami bezprzewodowymi.
- *Security*. Ustawienia bezpieczeństwa dla autoryzacji klientów bezprzewodowych i szyfrowania danych przesyłanych drogą radiową.
- *IEEE 802.1x/RADIUS*. Opcje dla lepszej ochrony: IEEE 802.1x Port-Based Network Access Control oraz uwierzytelnianie RADIUS (Remote Authentication Dial-In User Service).

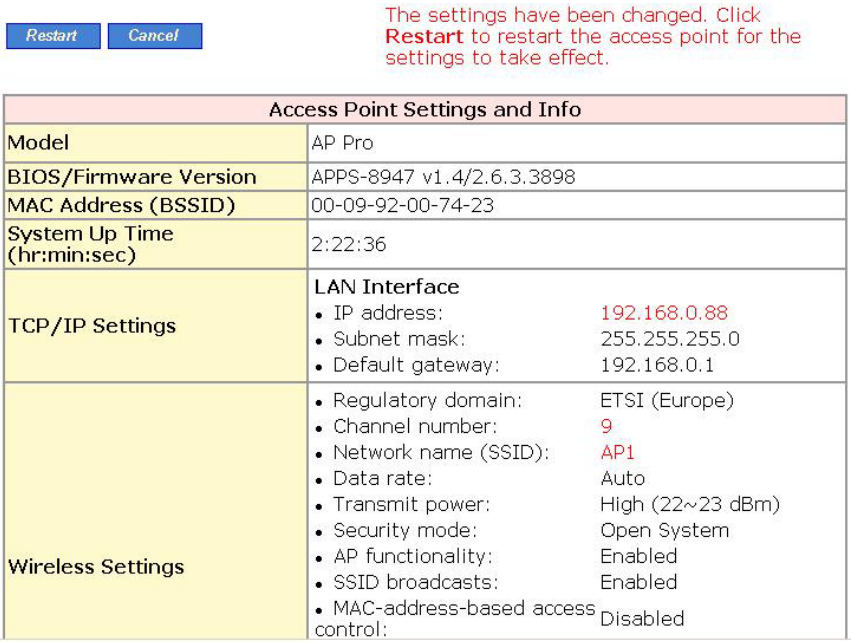
Advanced. Zaawansowane ustawienia punktu dostępowego.
- *Management*. Ustawienia UPnP i SNMP.

3.1.2 Komendy: Zapisz, Zapisz i Zresetuj, Anuluj

Rys. 9. Zapisz, Zapisz i Zresetuj, Anuluj.

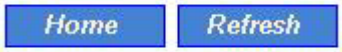
Na dole każdej strony zawierającej ustawienia, które są konfigurowalne, znajdują się trzy przyciski: Save, Save & Restart oraz Cancel. Kliknięcie na Save wprowadza zmienione ustawienia do pamięci punktu dostępowego i przenosi na stronę główną. Kliknięcie na Save & Restart wprowadza zmienione ustawienia do pamięci punktu dostępowego i natychmiast restartuje urządzenie, aby wprowadzone zmiany odniosły skutek. Kliknięcie na Cancel powoduje anulowanie wszelkich zmian w ustawieniach i powrót do strony głównej.

Podczas kliknięcia na Save, strona startowa zaakcentuje fakt wprowadzenia zmian w ustawieniach wyświetlając dwa przyciski: Restart i Cancel. Dodatkowo zmiany są podświetlone na czerwono. Kliknięcie na Cancel powoduje anulowanie wszystkich wprowadzonych zmian. Klikniecie na Restart restartuje urządzenie, aby zmiany zostały wprowadzone.



Rys. 10. Ustawienia, które zostały zmienione.

3.1.3 Komendy Powrót i Odśwież



Rys. 11. Powrót i Odśwież.

Na dole każdej strony, która wyświetla informacje tylko do odczytu znajdują się dwa przyciski: Home i Refresh. Kliknięcie na Home przenosi na stronę główną. Kliknięcie na Refresh odświeża wyświetlane informacje.

3.2 Status urządzenia

3.2.1 Podłączeni klienci bezprzewodowi

Wireless Clients Status

No.	MAC Address	IP Address	Name	Tx bytes	Rx bytes	Last activity time
1	00-06-F4-00-4C-50	192.168.168.3		322410	42149	00h:22m:24s

Rys. 12. Status przyłączonych klientów bezprzewodowych.

Na tej podstronie wyświetlają się informacje o każdym dołączonym kliencie: jego adres MAC i IP, nazwa użytkownika (jeśli klient jest autoryzowany przez IEEE 802.1x), liczba bajtów wysłanych i odebranych oraz czas ostatniej aktywacji.

3.2.2 Aktualny stan DHCP

DHCP Mapping Table

No.	MAC Address	IP Address	Type
1	00-60-B3-71-0F-07	192.168.0.2	Dynamic
2	00-06-F4-00-B8-19	192.168.0.88	Static

Rys. 13. Aktualne powiązania DHCP.

Na tej podstronie wyświetlane są wszystkie aktualne powiązania DHCP: statyczne i dynamiczne. Powiązania DHCP obrazują związek między adresem IP przypisanym przez serwer DHCP danego urządzenia a komputerem lub urządzeniem, które ten adres otrzymały. Komputer lub urządzenie będące klientem DHCP jest identyfikowane na podstawie własnego adresu MAC.

Statyczne powiązania wskazują, że dany klient DHCP zawsze otrzymuje określony adres IP z serwera DHCP. Statyczne powiązania DHCP możesz ustawić w sekcji Static DHCP Mappings na stronie konfiguracyjnej DHCP Server (zobacz dział 3.4.2). Dynamiczne powiązania pokazują, jak serwer DHCP wybiera adres IP z dostępnej puli adresowej określonej pierwszym adresem (First allocateable IP adress) oraz liczbą dostępnych adresów (Allocateable IP adress Mount), które można określić na stronie konfiguracyjnej DHCP Server.

3.3 Operacje ogólne

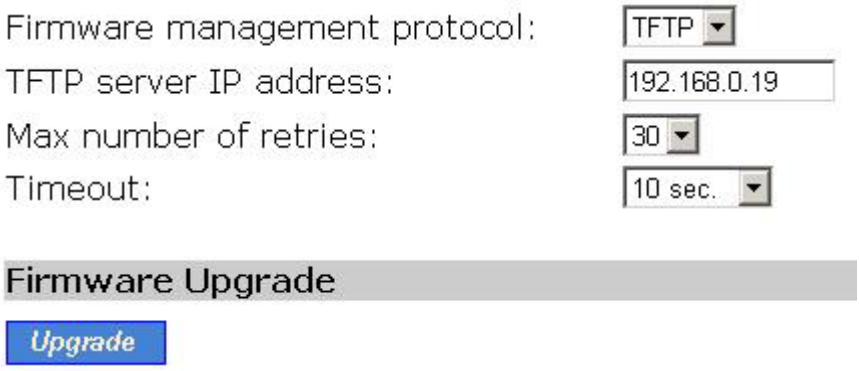
3.3.1 Zmiana hasła

Rys. 14. Hasło.

Na tej stronie można zmienić nazwę użytkownika i hasło dające prawo modyfikowania konfiguracji urządzenia. Nowe hasło należy wpisać dwa razy w celu jego potwierdzenia.

3.3.2 Zarządzanie firmware'm

3.3.2.1 Aktualizacja oprogramowania (firmware'u)



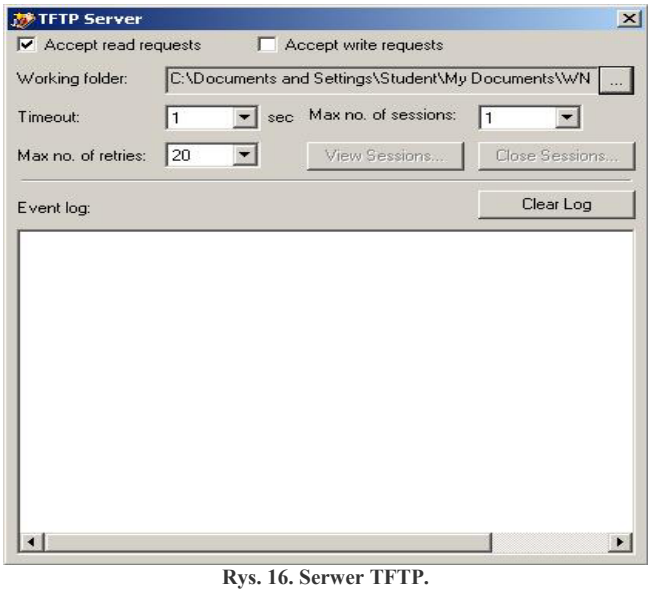
Rys. 15. Aktualizacja oprogramowania.

Punkt dostępowy może ściągać zaktualizowane oprogramowanie z określonego serwera TFTP. Na tej podstronie można wpisać adres IP określonego serwera TFTP, a następnie nakazać urządzeniu rozpoczęcie pobierania pliku.

W folderze "Utilities" na załączonym dysku CD znajduje się program TFTP Server (TftpSrvr.exe) do aktualizacji oprogramowania (firmware'u). Po uruchomieniu tego programu na komputerze, będzie on służył jako serwer TFTP.

Aby zaktualizować oprogramowanie punktu dostępowego należy:

1. Przygotować komputer, który będzie służył jako serwer TFTP oraz komputer zarządzający procesem aktualizacji.
2. Podłączyć ten komputer kablem krosowym do ethernetowego portu LAN/CONFIG urządzenia.
3. Ustawić adres IP komputera, aby należał do tej samej podsieci co punkt dostępowy.
4. Na komputerze uruchomić program TFTP Server i wskaż folder, w którym znajdują się pliki nowszego oprogramowania.
5. Na komputerze uruchomić przeglądarkę internetową i kliknąć na link General, Firmware Tools.
6. W sekcji Firmware Upgrade określić adres IP komputera będącego serwerem TFTP. Jeśli nie jest znany adres IP komputera, należy otworzyć okno poleceń i wpisać IpConfig, a następnie wciśnąć Enter.
7. Zatwierdzić proces aktualizacji klękając na Upgrade.



Rys. 16. Serwer TFTP.

UWAGA: Należy upewnij się, że opcja Accept read requests jest zaznaczona.

WSKAZÓWKA: Bardziej wygodny do aktualizacji oprogramowania punktu dostępowego jest Kreator Aktualizacji Oprogramowania (Firmware Upgrade Wizard) w programie Wireless Network Manager.

UWAGA: Po pojawieniu się okienka dialogowego programu TFTP server, upewniić się, że we wskazanym katalogu znajdują się pliki nowszego oprogramowania.

UWAGA: Adres IP punktu dostępowego i adres IP serwera TFTP muszą należeć do tej samej podsieci, aby TFTP działało.

UWAGA: Ze względu na niestabilną naturę fal radiowych, jest wysoce zalecane, by serwer TFTP i punkt dostępowy, którego oprogramowanie ma być zaktualizowane, były połączone siecią Ethernet, najlepiej w tej samej sieci lokalnej. Wtedy aktualizacja powinna przebiegać bezproblemowo.

UWAGA: Po aktualizacji oprogramowania należy skasować zawartość pamięci podręcznej (cache'u) przeglądarki internetowej, aby strony zarządzania przez internet wyświetlały się poprawnie.

UWAGA: Nieudana aktualizacja może zniszczyć oprogramowanie punktu dostępowego uniemożliwiając jego dalsze działanie. W takim przypadku należy skontaktować się z pomoc techniczną.

3.3.3 Archiwizacja i przywracanie ustawień konfiguracyjnych

Rys. 17. Zapisywanie/Przywracanie konfiguracji.

Punkt dostępowy może przesłać swoje ustawienia konfiguracyjne na serwer TFTP, aby zostały one zapisane do pliku. Później plik ten może zostać przywrócony z serwera TFTP do punktu dostępowego. Po więcej informacji o użytkowaniu narzędzia TFTP Server powiązanego z punktem dostępowym należy zajrzećdo poprzedniego rozdziału.

Aby zrobić kopię zapasową konfiguracji punktu dostępowego należy:

1. Przygotować komputer, który będzie służył jako serwer TFTP oraz komputer zarządzający procesem aktualizacji.
2. Podłączyć ten komputer kablem krosowanym do ethernetowego portu LAN/CONFIG urządzenia.
3. Ustawić adres IP komputera, aby należał do tej samej podsieci co punkt dostępowy.
4. Na komputerze uruchomić program TFTP Server, zaznacz opcję Accept write requests i określić folder, w którym mają być zapisane ustawienia konfiguracyjne.
5. Na komputerze uruchomić przeglądarkę internetową i kliknij na link General, Firmware Tools.
6. W sekcji Configuration Backup/Restoring określić adres IP komputera będącego serwerem TFTP. Jeśli nie jest znany adres IP komputera, otwórzyć okno poleceń i wpisać IpConfig, następnie wciśnij Enter.
7. Zatwierdzić proces tworzenia kopii zapasowej klikając na Backup. Ustawienia konfiguracyjne punktu dostępowego zostaną zapisane na serwerze TFTP jako "AaBbCcDdEeFf.hex", gdzie AaBbCcDdEeFf jest adresem MAC punktu dostępowego. Np., jeśli adres MAC urządzenia wynosi 00-01-01-33-44-55, to plik z zapisem konfiguracji będzie się nazywał: "000101334455.hex".

UWAGA: Należy pamiętać o włączeniu opcji Accept write requests w programie TFTP Server.

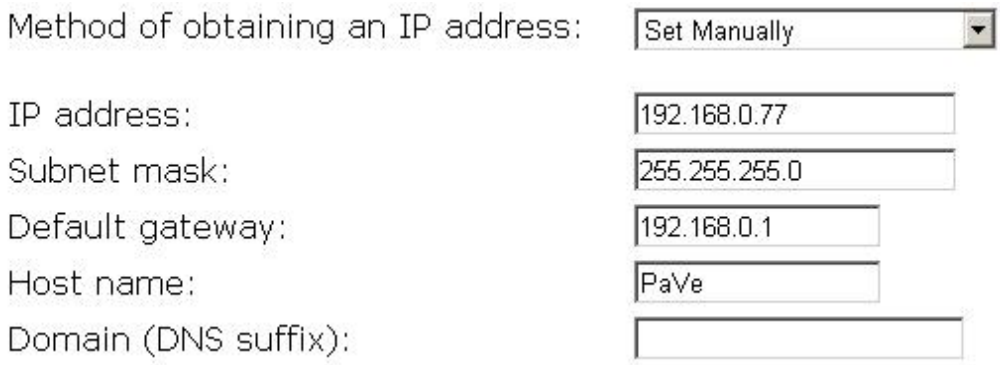
Aby przywrócić konfigurację punktu dostępowego:

1. Przygotować komputer, który będzie służył jako serwer TFTP oraz komputer zarządzający procesem aktualizacji.
2. Podłączyć ten komputer kablem krosowym do ethernetowego portu LAN/CONFIG urządzenia.
3. Ustawić adres IP komputera, aby należał do tej samej podsieci co punkt dostępowy.
4. Na komputerze uruchomić program TFTP Server i określ folder, w którym znajdują się pliki kopii zapasowej. Ich nazwą jest najczęściej adres MAC punktu dostępowego. Np., jeśli adres MAC urządzenia wynosi 00-01-01-33-44-55, to plik z zapisem konfiguracji będzie się nazywał: “000101334455.hex”.
5. Na komputerze uruchomić przeglądarkę internetową i kliknij na link General, Firmware Tools.
6. W sekcji Configuration Backup/Restoring określić adres IP komputera będącego serwerem TFTP. Jeśli nie znasz adresu IP komputera, otwórz okno poleceń i wpisz IpConfig, następnie wciśnij Enter.
7. Zatwierdzić proces przywracania konfiguracji z kopii zapasowej klikając na Restore. Następnie punkt dostępowy powinien skopiować plik konfiguracyjny z serwera TFTP.

UWAGA: Należy upewnić się, że wskazany plik jest kopią zapasową konfiguracji punktu dostępowego.

3.4 Konfigurowanie ustawień powiązanych z TCP/IP

3.4.1 Adresacja

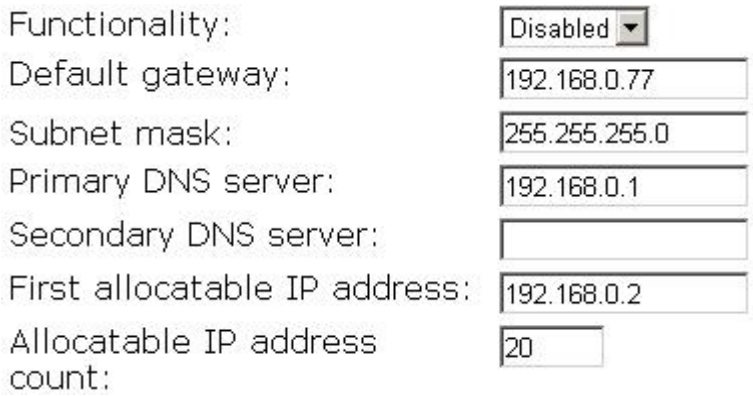


Rys. 18. Ustawienia TCP/IP.

Adres IP punktu dostępowego może być przydzielony ręcznie lub automatycznie z serwera DHCP w sieci LAN. Jeśli ręcznie ustawia się adres IP, maskę podsieci i bramę domyślną, należy ustawić je tak, by zgadzały się z otoczeniem sieci LAN. Dodatkowo możesz określić nazwę hosta, i domeny (DNS suffix).

3.4.2 Serwer DHCP

3.4.2.1 Podstawy

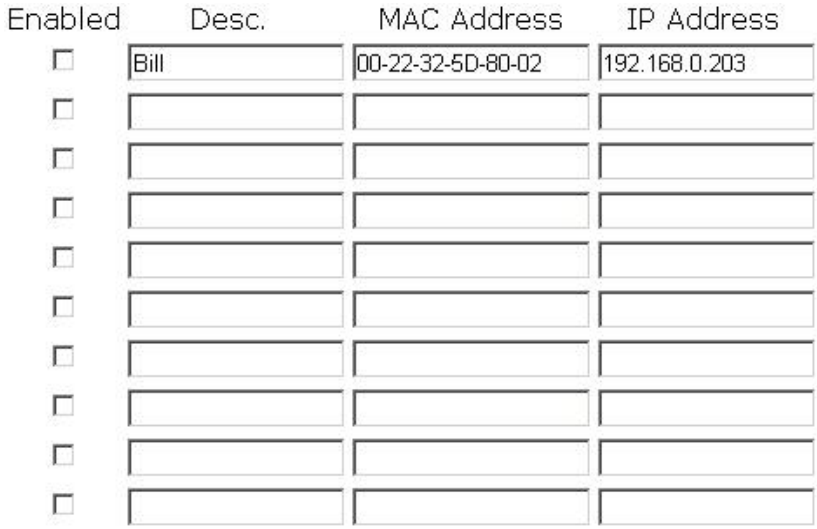


Rys. 19. Podstawowe ustawienia serwera DHCP.

Punkt dostępowy dzięki DHCP może automatycznie przydzielać adresy IP komputerom-klientom. W tej sekcji stron zarządzania można określić: bramę domyślną, maskę podsieci, pierwszy serwer DNS i drugi serwer DNS; ustawienia te będą wysyłane do klienta na jego żądanie. Dodatkowo można określić pierwszy adres IP, który będzie przydzielony klientowi oraz liczbę alokowanych adresów IP.

UWAGA: W sieci LAN powinien być tylko jeden serwer DHCP; w przeciwnym wypadku DHCP może pracować niepoprawnie. Jeśli w sieci LAN jest już serwer DHCP, wyłącz funkcję serwera DHCP w punkcie dostępowym.

3.4.2.2 Statyczne powiązania DHCP



Rys. 20. Statyczne powiązania DHCP.

Adresy IP serwerów są najczęściej statyczne, aby klienci mogli zawsze zlokalizować je po stałym adresie IP. Dzięki funkcji Static DHCP Mappings można zapewnić hostowi ten sam adres IP z serwera DHCP, gdy tylko o to poprosi. Dlatego zamiast przypisywać adres IP serwera intranetowego ręcznie, można go skonfigurować tak, by otrzymywał adres z DHCP i zawsze posiadał ten sam adres IP.

Aby zawsze przypisać statyczny adres IP danemu klientowi należy:

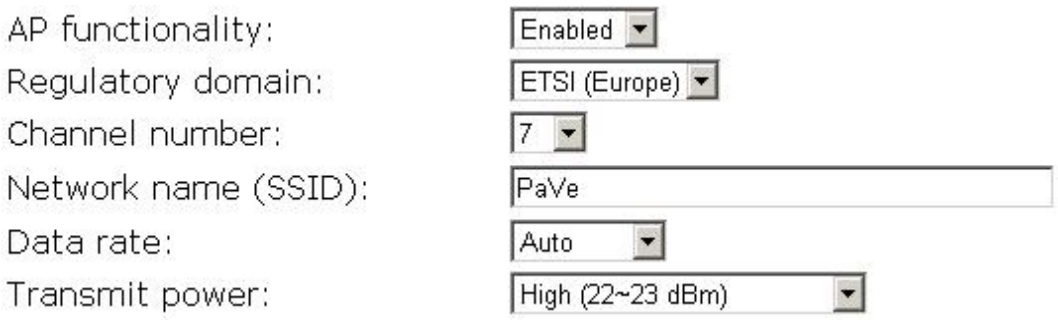
1. Określić adres MAC klienta DHCP, a adres IP zostanie do niego przypisany. Następnie daj opis do tego powiązania.
2. Zaznaczyć odpowiednią opcję (check box) jako Enabled.

3.5 Konfigurowanie ustawień powiązanych z IEEE 802.11b

3.5.1 Komunikacja

3.5.1.1 Podstawy

Ustawienia powiązane z IEEE 802.11b zawierają: AP functionality (funkcja punktu dostępowego), Regulatory domain (regulacje prawne), Channel number (numer kanału), Network name (SSID) (nazwa sieci), Data rate (prędkość transmisji) i Transmit power (moc nadajnika).



Rys. 21. Podstawowe ustawienia komunikacyjne IEEE 802.11b.

Dla specyficznych potrzeb, jak konfiguracja punktu dostępowego jako mostu między dwoma sieciami LAN, funkcja punktu dostępowego może być wyłączona, aby żaden z klientów bezprzewodowych nie mógł połączyć się z urządzeniem.

Liczba dostępnych kanałów radiowych (RF) zależy od lokalnych uregulowań prawnych; dlatego należy wybrać odpowiednią opcję z menu Regulatory domain, tak by zgadzała się z lokalnymi regulacjami. Identyfikator SSID klienta bezprzewodowego i SSID punktu dostępowego powinny być identyczne, aby oba urządzenia mogły się wzajemnie komunikować.

Moc nadawania modułu radiowego urządzenia może być zmieniana tak, by zmieniać pokrycie radiowe punktu dostępowego i dostosować się do uwarunkowań prawnych w obrębie danego kraju. W Polsce max. moc e.i.r.p. wypromieniowana nie może przekroczyć 100mW, czyli 20 dB.

UWAGA: Przy ustawieniach kanału dla innych anten niż te, które dostarczył producent urządzenia, warto ustalić kanał najefektywniejszy. Zazwyczaj jest to kanał 7, ale szczegółowe dane określają producenci anten.

3.5.1.2 Równoważenie obciążenia punktu dostępowego

Rys. 22. Ustawienia równoważenia obciążenia punktu dostępowego.

Niektóre punkty dostępowe mogą tworzyć tzw. grupy równoważenia obciążenia, jeśli należą do tego samego Group ID. Metoda równoważenia obciążenia (load balancing) może występować w dwóch ‘opcjach‘:

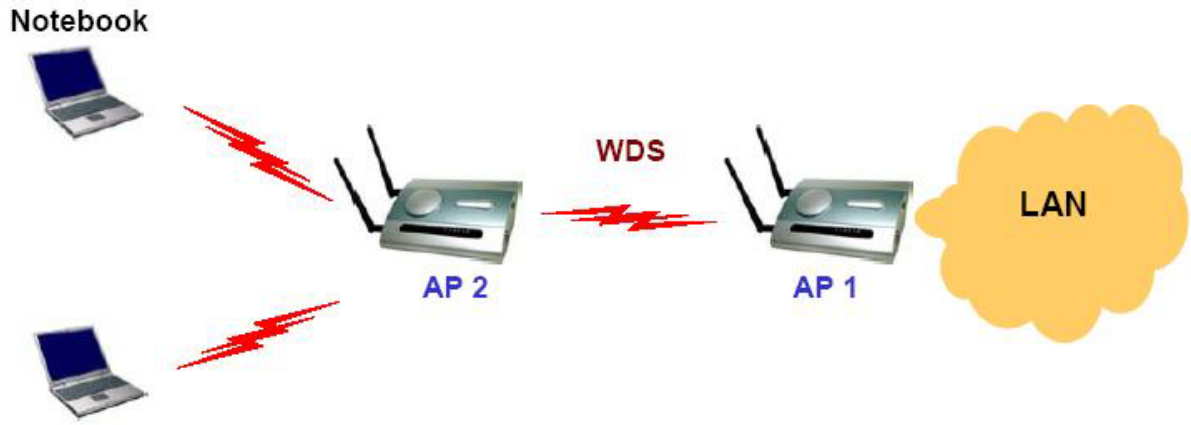
1. Number of Users (liczba użytkowników)

lub

2. Traffic Load (obciążenie ruchem).

Jeśli wybrany został algorytm oparty na liczbie użytkowników, nowy klient bezprzewodowy może podłączyć się tylko do tego punktu dostępowego, który ma najmniej dołączonych użytkowników w grupie. Z drugiej strony, jeśli algorytm opiera się na analizie obciążenia ruchu w sieci, nowy klient bezprzewodowy może podłączyć się tylko do punktu dostępowego, który ma najmniejsze obciążenie ruchem sieciowym w grupie.

3.5.1.3 WDS (Wireless Distribution System)

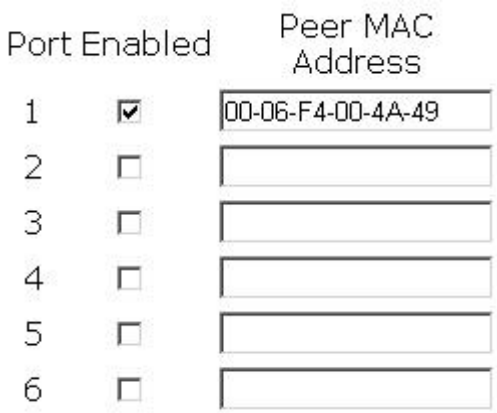


Rys. 23. Wireless Distribution System.

Tradycyjnie punkt dostępowy podłączany jest do sieci Ethernet. Dzięki systemowi Wireless Distribution System (WDS) punkty dostępowe mogą komunikować się między sobą. Na Rys. 23. **AP 2** pracuje jako punkt dostępowy dla notebooków i przesyła ich pakiety do **AP 1** poprzez WDS. Następnie **AP 1** przesyła pakiety do sieci LAN. Pakiety

przeznaczone dla notebooków odbywają odwrotną drogę: z sieci LAN poprzez punkty dostępowe AP 1 i 2 do notebooków. W tym przypadku urządzenie AP 2 odgrywa rolę "AP repeatera" (wzmacniacza).

UWAGA: Punkt dostępowy może posiadać do sześciu linków WDS łączących z innymi punktami dostępowymi lub bezprzewodowymi mostami.

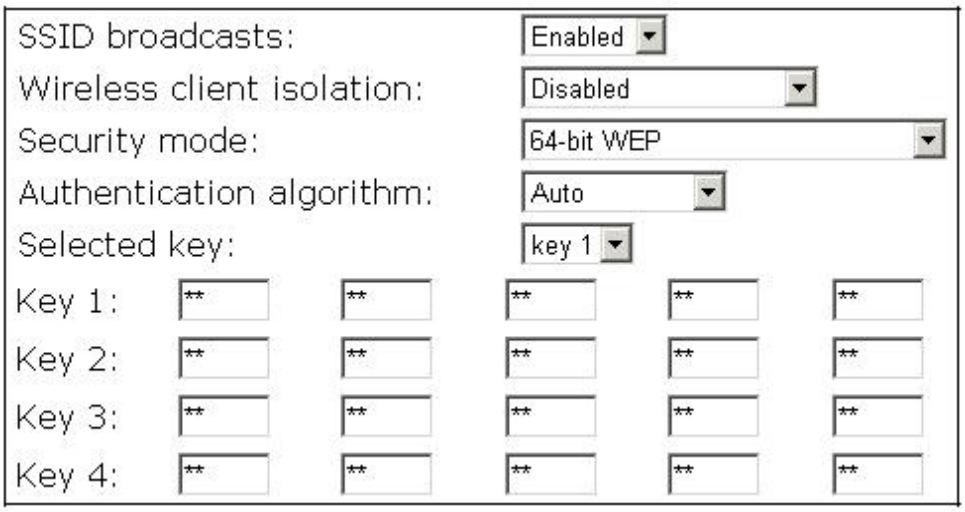


Rys. 24. Ustawienia WDS.

Aby włączyć połączenie WDS należy:
1. Określić adres MAC urządzenia na drugim końcu linku WDS.
2. Zaznaczyć odpowiednią opcję (check box) Enabled.

Np. wymagane jest połączenie linkiem WDS dwóch punktów dostępowych, których adresy MAC wynoszą: 00-02-65-01-62-C5 i 00-02-65-01-62-C6. Na urządzeniu 00-02-65-01-62-C5 należy ustawić adres MAC na porcie pierwszym na 00-02-65-01-62-C6, na urządzeniu 00-02-65-01-62-C6 należy wpisać adres MAC na porcie pierwszym jako 00-02-65-01-62-C5.

3.5.2 Bezpieczeństwo



Rys. 25. Podstawowe ustawienia bezpieczeństwa IEEE 802.11b.

Ustawienia bezpieczeństwa IEEE 802.11b zawierają:
- SSID broadcasts (rozgłaszanie SSID),
- Wireless client isolation (izolację klientów radiowych),
- Security mode (tryb zabezpieczenia),
- IEEE 802.11 Authentication algorithm (algorytm autoryzacji IEEE 802.11),
- WEP keys (klucze WEP - Wired Equivalent Privacy),
- MAC address control (dostęp do sieci poprzez weryfikację adresów MAC).

Z powodów bezpieczeństwa wysoce zalecane jest, by tryb zabezpieczenia ustawiony był na inny niż Open System (system otwarty). Gdy tryb zabezpieczenia ustawiony jest na Open System, nie jest dokonywana żadna autoryzacja czy szyfrowanie danych. Dodatkowo można wyłączyć (disable) funkcję rozgłaszania SSID, by klient radiowy z SSID ustawionym na "any" nie mógł podłączyć się do punktu dostępowego.

Kiedy opcja Wireless client isolation (ADV+) jest ustawiona na This AP only (tylko ten punkt dostępowy), klienci bezprzewodowi tego punktu dostępowego nie widzą się wzajemnie, a ruch "międzyradiowy" jest zablokowany. Gdy ustawiona jest opcja All APs in this Subnet (wszystkie punkty dostępowe w tej podsieci), ruch pomiędzy klientami radiowymi różnych punktów dostępowych tej samej podsieci jest zablokowany. Ta cecha jest użyteczna dla sieci WLAN umieszczonych w miejscach publicznych. Dzięki temu hackerzy nie mają szans na atak innych radiowych użytkowników hotspota (publicznego punktu dostępowego).

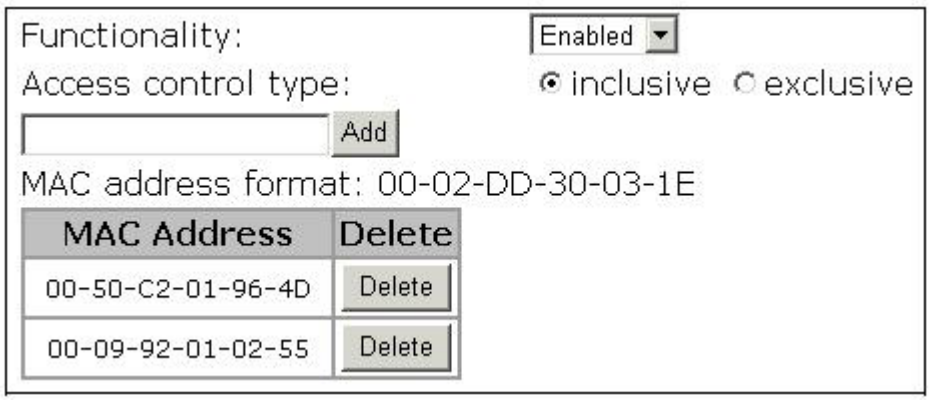
Proponuje się dziewięć trybów zabezpieczeń w zależności od modelu urządzenia:
- **Open System**. Brak autoryzacji i szyfrowania danych.
- **64-bit WEP**. Autoryzacja i szyfrowanie danych oparte na 64-bit WEP (Wired Equivalent Privacy).
- **128-bit WEP**. Autoryzacja i szyfrowanie danych oparte na 128-bit WEP (Wired Equivalent Privacy), używane są klucze 128 bitowe.

W tym sześć trybów zabezpieczeń w modelach: Advanced lub Advanced+ :
- **802.1x EAP-MD5**. Włączona jest funkcja IEEE 802.1x oraz używana autoryzacja EAP-MD5 opartej na nazwie użytkownika i haśle. Brak szyfrowania danych.
- **802.1x EAP-MD5 + 64-bit WEP**. Włączona jest funkcja IEEE 802.1x oraz używana autoryzacja EAP-MD5 opartej na nazwie użytkownika i haśle. Szyfrowanie danych oparte na 64-bit WEP.
- **802.1x EAP-MD5 + 128-bit WEP**. Włączona jest funkcja IEEE 802.1x oraz używana autoryzacja EAP-MD5 opartej na nazwie użytkownika i haśle. Szyfrowanie danych oparte na 128-bit WEP.
- **802.1x EAP-TLS; no encryption**. Włączona jest funkcja IEEE 802.1x oraz używana autoryzacja użytkownika EAP-TLS (Transport Layer Security) opartej na certyfikatach cyfrowych. Brak szyfrowania danych.
- **802.1x EAP-TLS 64-bit key**. Włączona jest funkcja IEEE 802.1x oraz używana autoryzacja użytkownika oraz szyfrowanie danych EAP-TLS opartej na certyfikatach cyfrowych. Klucze sesji są 64-bitowe.
- **802.1x EAP-TLS 128-bit key**. Włączona jest funkcja IEEE 802.1x oraz używana autoryzacja użytkownika oraz szyfrowanie danych EAP-TLS opartej na certyfikatach cyfrowych. Klucze sesji są 128-bitowe.

Zgodnie ze standardem IEEE 802.11 funkcja WEP może być używana do autoryzacji i szyfrowania danych. Standardowo autoryzacja Shared Key jest używana, gdy włączone jest szyfrowanie danych WEP. W rzadkich przypadkach może być używana autoryzacja Open System, gdy szyfrowanie danych WEP jest włączone. Opcje Authentication algorithm (algorytm autoryzacji) zostały wprowadzone dla lepszej zgodności klientów bezprzewodowych z różnymi rodzajami kart sieciowych WLAN. Są dostępne trzy opcje: Open System, Shared Key oraz Auto.

W dziale 3.5.3 znajduje się więcej informacji o standardzie IEEE 802.1x.

UWAGA: Każde pole ustawień klucza WEP jest liczbą szesnastkową z zakresu 00 do FF. Np., gdy tryb zabezpieczenia ustawiony jest na 64-bit WEP, można ustawić klucz pierwszy (Key 1) na "00 01 2E 3A DF".



Rys. 26. Ustawienia kontroli dostępu opartej na adresach MAC.

Dzięki funkcji MAC-Address-Based Access Control można określić czy dany komputer bezprzewodowy może czy nie

może podłączyć się do punktu dostępowego. Gdy typ tablicy ustawiony jest na inclusive, wpisy do tablicy są dopuszczone do połączenia się z punktem dostępowym. Gdy typ tablicy ustawiony jest na exclusive, wpisy do tablicy nie są dopuszczane do połączenia się z punktem dostępowym.

Aby zabronić klientowi bezprzewodowemu dostępu do sieci radiowej należy:

1. Wybierać *Enabled* z rozwijalnej listy przy opcji *Functionality*.
2. Ustawić *Access Control* type na *exclusive*.
3. Określić adres *MAC* klienta, który ma być zablokowany i kliknij *Add* (dodaj).
4. Powtarzać Krok 3. dla innych klientów radiowych.

Aby przydzielić klientowi bezprzewodowemu dostęp do sieci radiowej należy:

1. Wybrać *Enabled* z rozwijalnej listy przy opcji *Functionality*.
2. Ustawić *Access Control* type na *inclusive*.
3. Określić adres *MAC* klienta, który ma otrzymać dostęp i kliknij *Add* (dodaj).
4. Powtarzać Krok 3. dla innych klientów radiowych.

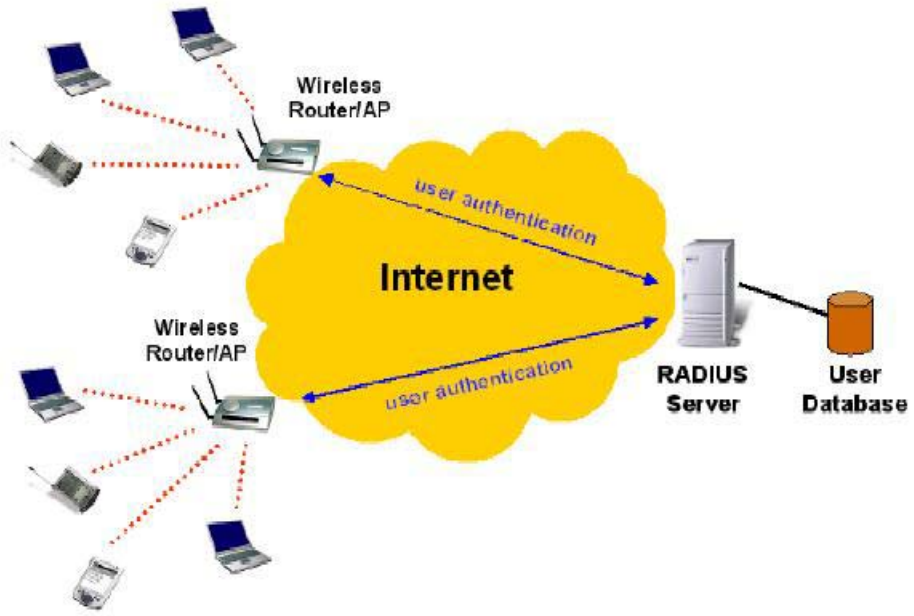
Aby skasować dowolny wpis z tabeli kontroli dostępu należy

Kliknąć przycisk *Delete* (usuń) znajdujący się obok wpisu.

3.5.3 IEEE 802.1x/RADIUS

IEEE 802.1x Port-Based Network Access Control jest nowym standardem rozwiązującym niektóre zagadnienia bezpieczeństwa związane z IEEE 802.11 takie, jak brak autoryzacji opartej na użytkowniku i dynamicznej dystrybucji kluczy szyfrujących. Dzięki IEEE 802.1x i wspomaganiu serwera RADIUS (Remote Authentication Dial-In User Service) oraz bazy danych dołączonych użytkowników, firma lub ISP (Internet Service Provider) może zarządzać dostępem do radiowej sieci LAN jej mobilnych użytkowników. Przed uzyskaniem dostępu do radiowej sieci LAN wspierającej IEEE 802.1x, użytkownik musi okazać swoją nazwę użytkownika i hasło lub cyfrowy certyfikat do końcowego serwera RADIUS poprzez protokół EAPOL (Extensible Authentication Protocol Over LAN). Serwer RADIUS może zapisywać informacje o połączeniu, jak: czas zalogowania i wylogowania użytkownika bezprzewodowej sieci LAN w celu prowadzenia monitoring lub bilingu.

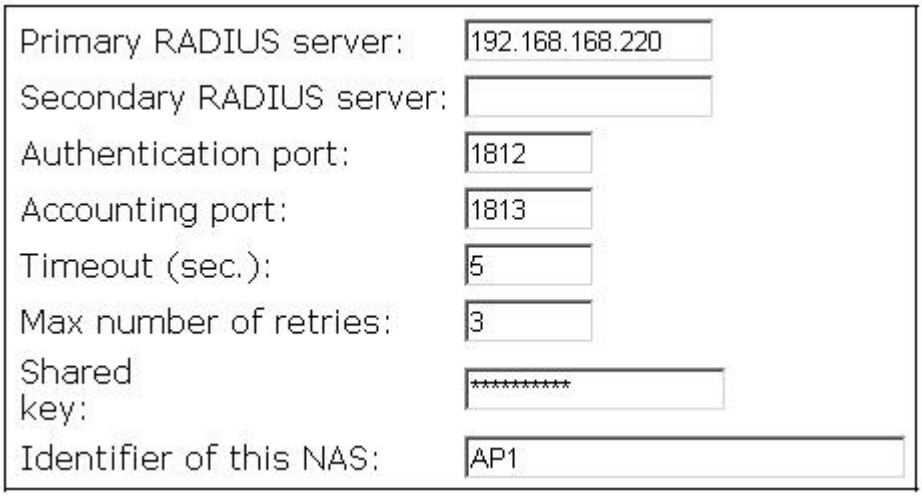
Funkcję IEEE 802.1x punktu dostępowego można kontrolować poprzez security mode (zobacz Rozdział 3.5.2). Tak więc radiowy punkt dostępowy wspiera dwa mechanizmy autoryzacji - EAP-MD5 (Message Digest version 5), EAP-TLS (Transport Layer Security). Jeśli jest używany EAP-MD5, użytkownik w celu autoryzacji musi podać swoją nazwę użytkownika oraz hasło. Gdy używa się EAP-TLS, komputer-klient w celu autoryzacji automatycznie prześle cyfrowy certyfikat użytkownika, który zapisany jest na dysku twardym komputera lub karcie pamięci typu smart card. Po udanej autoryzacji EAP-TLS automatycznie jest generowany klucz sesji do szyfrowania radiowych pakietów przesyłanych między bezprzewodowym klientem a przypisanym mu radiowym punktem dostępowym. Podsumowując - EAP-MD5 wspiera tylko autoryzację użytkownika, podczas gdy EAP-TLS wspiera autoryzację użytkownika, jak i dynamiczną dystrybucję klucza szyfrującego.



Rys. 27. IEEE 802.1x i RADIUS.

Punkt dostępowy wspierający IEEE 802.1x może być skonfigurowany do komunikacji z dwoma serwerami RADIUS. Kiedy pierwszy serwer RADIUS nie odpowiada, punkt dostępowy próbuje skomunikować się z drugim serwerem RADIUS. Można określić czas oczekiwania na odpowiedź serwera (tzw. timeout) i liczbę prób nawiązania połączenia z serwerem pierwszym, zanim nastąpi połączenie z drugim serwerem RADIUS.

Radiowy punkt dostępowy wspierający IEEE 802.1x i jego serwer(y) RADIUS dzielą tajny klucz, którym identyfikują się wzajemnie. Dodatkowo, prócz adresu IP, bezprzewodowy punkt dostępowy może identyfikować się nazwą NAS (Network Access Server). Każdy radiowy punkt dostępowy wspierający IEEE 802.1x musi posiadać unikatowy identyfikator NAS.



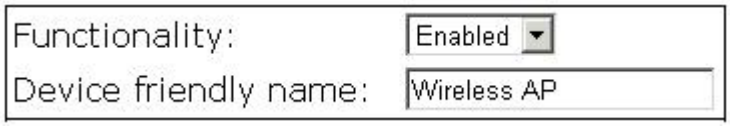
Rys. 28. Ustawienia IEEE 802.1x/RADIUS.

WSKAZÓWKA: Więcej informacji o tworzeniu bezpiecznych sieci WLAN wspierających IEEE 802.1x można znaleźć w dokumentacji tego standardu na załączonej płycie CD.

3.6 Konfigurowanie ustawień zaawansowanych

3.6.1 Zarządzanie

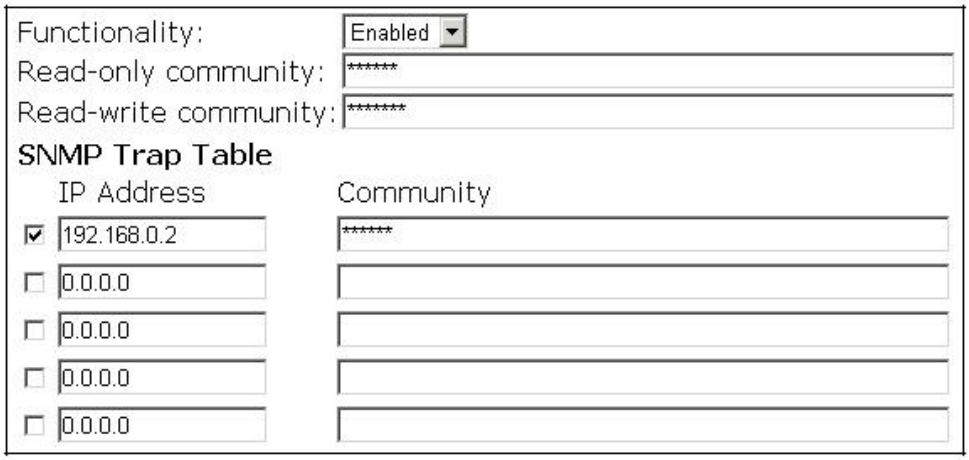
3.6.1.1 UPnP



Rys. 29. Ustawienia UPnP.

UPnP (Universal Plug and Play) pozwala użytkownikowi Windows XP na automatyczne wykrywanie urządzeń peryferyjnych przez HTTP. Gdy funkcja UPnP jest włączona, można zobaczyć punkt dostępowy w ‘Moich miejscach sieciowych‘ Windows XP. Urządzeniu można nadać przyjazną nazwę, pod którą będzie wyświetlane w ‘Moich miejscach sieciowych’. Podwójne kliknięcie na ikonę w ‘Moich miejscach sieciowych’ reprezentującą punkt dostępowy uruchomi domyślną przeglądarkę sieciową ze stroną konfiguracji urządzenia.

3.6.1.2 SNMP



Rys. 30. Ustawienia SNMP.

Funkcja SNMP (Simple Network Management Protocol) może być wyłączona i można określić nazwę (użytą jako hasło) środowiska tylko do odczytu i odczytaj-zapisz. Dodatkowo można ustawić do pięciu pułapek SNMP w SNMP Trap Table. Punkt dostępowy udostępnia następujące typy pułapek: Cold Start, Warm Start, Link Up, link Down oraz SNMP Authentication Failure.

UWAGA: Błąd SNMP Authentication Failure pojawia się przy użyciu niepoprawnej nazwy (hasła) środowiska do zarządzania punktem dostępowym przez SNMP i SNMP MIB II OID; snmpEnableAuthenTraps jest włączone (domyślnie jest wyłączone).

Aby określić cel pułapki należy:

1. Wpisać adres IP hosta docelowego.
2. Wpisać Community (nazwę-hasło) dla hosta.
3. Zaznaczyć odpowiednią opcję (check box) obok miejsca z wpisanym adresem IP.

4 Załącznik A

4.1 A-1: Ustawienia domyślne

WSKAZÓWKA: W celu przywrócenia ustawień fabrycznych, należy skorzystać z przełącznika Default (SF-Reset lub Soft-Reset) urządzenia AP

Nazwa ustawienia	Wartość domyślna
Global	
User Name	root
Password	root
IEEE 802.11b	
Regulatory Domain	FCC (U.S.)
Channel Number	11
SSID	wireless
SSID Broadcasts	Enabled
Transmission Rate	11Mbps
Transmit Power	High

MAC Address	Adres MAC jest zapisany na karcie PCMCIA lub na spodniej części obudowy punktu dostępowego.
Security Mode	Open System
Selected WEP Key	Key #1
WEP Key #1	00-00-00-00-00
WEP Key #2	00-00-00-00-00
WEP Key #3	00-00-00-00-00
WEP Key #4	00-00-00-00-00
MAC-Address-Based Access Control	Disabled
Access Control Table Type	Inclusive
Wireless Client Isolation	Disabled
AP Load balancing	Disabled
LAN Interface	
Method of obtaining an IP Address	Set manually
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
Management	
UPnP	Enabled
SNMP	Enabled
SNMP read community	public
SNMP write community	private
Telnet	Enabled

4.2 A-2: Oznaczenia diod LED

Punkt dostępowy posiada kilka diod kontrolnych umieszczonych na obudowie. Każda z kontrolek ma inne znaczenie:
ALV: Alive. Miga, kiedy punkt dostępowy pracuje prawidłowo.
RF: interfejs IEEE 802.11b.
LAN: interfejs Ethernet LAN.
PWR: Zasilanie.

5 Załącznik B:

5.1 B-1: Usuwanie problemów

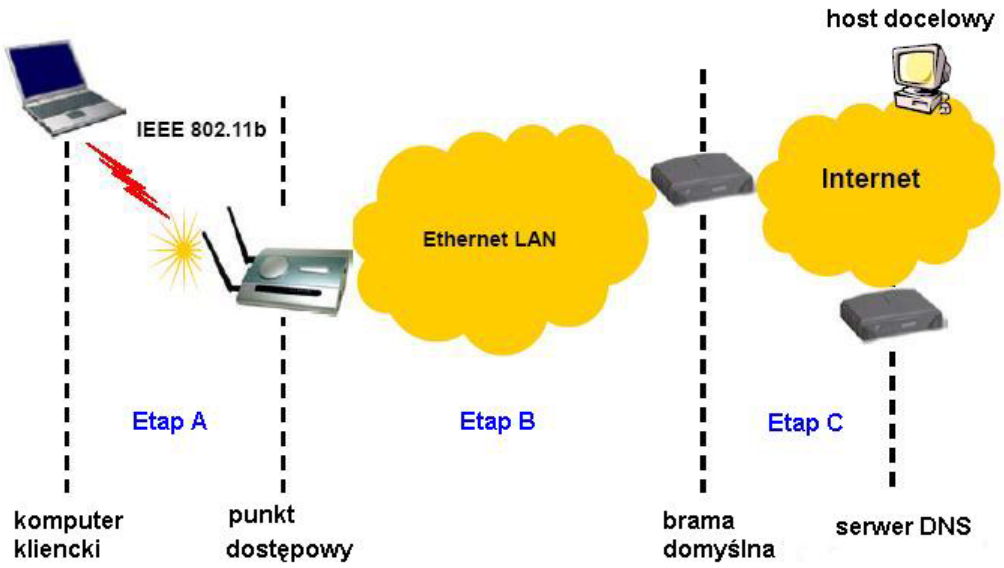
W przypadku wykrycia nieprawidłowego funkcjonowania punktu dostępowego w pierwszej kolejności należy:
Upewnić się, że zasilanie jest włączone, oraz że kabel zakończony wtykiem RJ-45 łączący urządzenie z siecią Ethernet jest prawidłowo podłączony.
Upewnić się, że dioda sygnalizacyjna ALV migocze sygnalizując prawidłową pracę punktu dostępowego.
Upewnić się, że kabel łączący punkt dostępowy z siecią Ethernet, spełnia wszystkie wymagania, co do jego typu. Pamiętaj, że kabel może być normalny lub krosowany.

5.2 B-2: Problemy ustawień sieci bezprzewodowych

Komputer kliencki nie może się połączyć z punktem dostępowym.

- Czy klient jest odpowiednio podłączony do sieci w trybie infrastruktury?
- Sprawdzić tryb działania na karcie sieciowej WLAN.
- Czy identyfikator SSID dla karty sieciowej WLAN jest identyczny, jak w przypadku punktu dostępowego?
- Sprawdzić SSID karty sieciowej WLAN oraz urządzenia dostępowego.
- Czy funkcja WEP (Wired Equivalent Privacy) odpowiedniego punktu dostępowego jest włączona?
- Upewnić się, że ustawienia bezpieczeństwa WEP dla komputera klienckiego są takie same, jak punktu dostępowego.
- Czy punkt dostępowy jest wystarczająco blisko, by nawiązać komunikację?
- Sprawdzić siłę sygnału i jakość połączenia oznaczonych przez pozycje signal strength and link quality dla karty sieciowej WLAN.

5.3 B-3: Problemy ustawień TCP/IP



Rys. 31. Etapy komunikacji łączenia klienta z hostem docelowym.

Dla umożliwienia bezprzewodowej komunikacji komputera klienckiego poprzez sieć Internet z komputerem docelowym (correspondent host), znajdującym się w domenie np. http//www.wi-fi.com w pierwszej kolejności jest wysyłane pytanie do internetowego serwera DNS. Najpierw pytanie trafia do punktu dostępowego AP, a następnie jest kierowane do bramy sieciowej, która to znajduje się w ustawieniach komputera klienckiego. Po przejściu przez bramę pytanie trafia do serwera DNS. Następnie serwer wyszukuje adres komputera, którego dotyczy pytanie (correspondent host) i wysyła odpowiedź z powrotem do komputera klienckiego używając tej samej drogi, którą przebył pakiet z pytaniem. Kiedy już komputer kliencki otrzyma odpowiedź od serwera DNS zawierającą adres IP komputera docelowego, wysyła pakiety, które zawierają już adres IP odbiorcy.
Tak jak pokazuje rysunek ścieżka używana do komunikacji, może zostać przerwana w czasie jednego z trzech etapów. Systemy operacyjne dostarczą program ping.exe. Jest to proste narzędzie diagnostyczne używane do wykrycia problemów w komunikacji.

UWAGA: Jeśli w komputerze klienckim są zainstalowane dwie lub więcej kart sieciowych, TCP/IP może pracować niewłaściwie ze względu na nieprawidłową tablicę routingu. Korekcja tablicy routingu może zostać przeprowadzona przy użyciu programu route.exe, umożliwiającego dodawanie lub kasowanie zapisów w tablicy routingu. W celu uniknięcia błędów można również użyć programu Device Manager do wyłączenia niepotrzebnych urządzeń (kart sieciowych).

Punkt dostępowy nie odpowiada na ping wysłany z komputera klienckiego.

- Czy dwie lub więcej kart jest zainstalowanych na jednym komputerze?
- Użyć route.exe do modyfikacji tablicy routingu.
- Użyć Device Manager (Menadżer urządzeń), aby wyłączyć zbędne karty sieciowe.
- Czy odpowiednie łącze (Ethernet lub IEEE 802.11b) jest zaimplementowane?
- Upewnić się, że łącze Ethernet działa poprawnie.
- Upewnić się, że ustawienia sieci bezprzewodowej dla komputera klienckiego i punktu dostępowego pasują do

siebie.

- Czy adres IP komputera klienckiego oraz adres IP punktu dostępowego mają tą samą maskę sieciową?
- Użyć WinIPCfg.exe lub IPConfig.exe dla odczytania bieżących ustawień IP komputera klienckiego. Upewnić się, że adresy IP klienta i punktu dostępowego mają taką samą maskę.

WSKAZÓWKA: W przypadku zapomnienia bieżących ustawień IP dla punktu dostępowego, należy użyć programu Wireless Router/AP Browser dla uzyskania tych informacji (Załącznik B-3).

Brama sieciowa komputera klienckiego nie odpowiada na ping wysyłany z komputera klienckiego.

- Rozwiązać najpierw wcześniejsze problemy.
- Czy adres IP dla punktu dostępowego oraz adres IP dla komputera klienckiego mają taką samą maskę?
- Jeśli nie można znaleźć żadnych nieprawidłowych ustawień punktu dostępowego, brama sieciowa może być w tym momencie odłączona lub też występują inne problemy w szkielecie sieci.

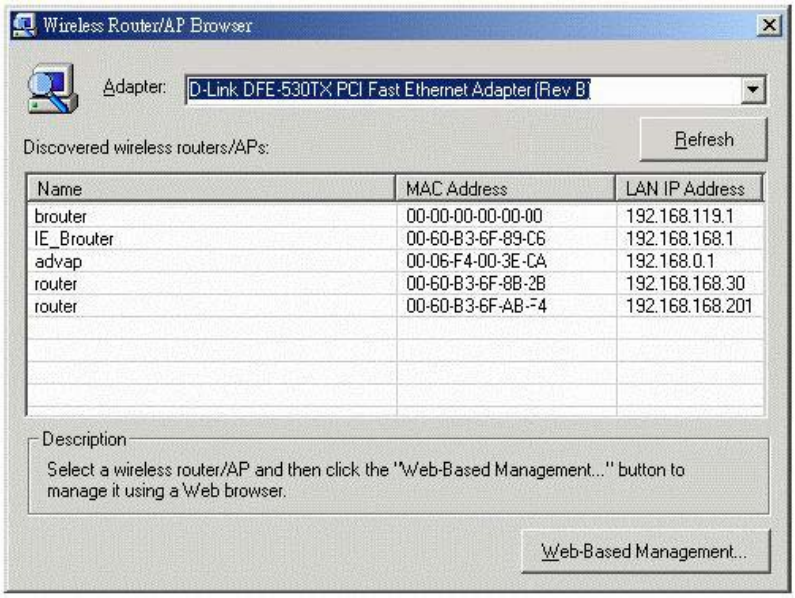
Serwer DNS, do którego komputer kliencki kieruje zapytania nie odpowiada na ping.

- Rozwiązać najpierw wcześniejsze problemy.
- Jeśli nie można znaleźć żadnych nieprawidłowych ustawień punktu dostępowego, serwer DNS może być w tym momencie odłączony lub też występują inne problemy w szkielecie sieci.

5.4 B-4: Nieznane problemy

Punkt dostępowy został skonfigurowany tak, że adres IP pobierany jest automatycznie z serwera DHCP. Jak można sprawdzić adres IP, który umożliwi zarządzanie urządzeniem przez przeglądarkę stron internetowych?

- Należy w tym celu użyć narzędzia Wireless Router/AP Browser (WLBrwsr.exe), które znajduje się w katalogu "Utilities" na dołączonej płycie CD. Program wykrywa najbliższy punkt dostępowy i pokazuje jego adres MAC oraz IP. Dodatkowo, program może uruchomić domyślną przeglądarkę na komputerze.



Rys. 32. Wireless Router/AP Browser.

Punkt dostępowy przestał działać i nie można nim zarządzać przez stronę WWW.

- Oprogramowanie sprzętowe może być zainstalowane na nieodpowiednim komputerze.
- Odłączyć punkt dostępowy od zasilania tak, by zrestartować urządzenie.
- Skontaktować się z działem technicznym, opisać problem i jeśli wynika on z nieprawidłowości oprogramowania, pomoże to w przyszłości uniknąć takich problemów.

Jeśli po restarcie punkt dostępowy wciąż nie działa, przyczyną awarii może być awaria jednego z komponentów urządzenia.

- W takim wypadku skontaktuj się z działem technicznym w celu dokonania naprawy.