

instrukcja obsługi routera VI-3223u

Wersja A2.03.0, 25 Kwiecień 2013



261099-00211

Wstęp

Instrukcja ta zawiera informacje o instalacji i działaniu urządzenia. Aby w pełni skorzystać z instrukcji wymagana jest podstawowa znajomość terminologii telekomunikacyjnej.

Informacje o produktach, nowe wersje urządzeń oraz poprawki instrukcji znajdziesz na naszej stronie: <http://www.orange.pl/>

Ważne instrukcje bezpieczeństwa

Następujące reguły postępowania są wskazane podczas rozpakowywania, instalacji oraz użytkowania twojego urządzenia elektronicznego.

- Aby uniknąć porażenia prądem, nie używaj, oraz nie instaluj tego urządzenia w pobliżu wody, na przykład blisko wanny, zlewu kuchennego, w pralni, blisko basenu. Nie umieszczaj urządzenia w miejscu narażonym na działanie deszczu lub wilgoci (np. wilgotna piwnica).
- Nie podłączaj przewodu zasilającego tak aby wisiał, lecz umieść go tak aby leżał swobodnie. Na jego drodze nie powinno być żadnych przeszkód, jak również nie powinny na nim leżeć żadne ciężkie przedmioty. Nie chodź po nim, nie deptaj i nie gnij przewodu.
- Używaj tylko przewodu zasilającego i zasilacza dostarczonego z urządzeniem.
- Aby zabezpieczyć urządzenie przed przegrzaniem upewnij się, że żaden otwór w obudowie nie jest zablokowany.
- Unikaj używania telefonu (z wyłączeniem bezprzewodowych) podczas burzy. Istnieje ryzyko porażenia podczas uderzenia błyskawicy. Nie używaj telefonu, do powiadomienia o wycieku gazu, będąc w pobliżu wycieku.
- Nigdy nie instaluj okablowania telefonicznego podczas pogody burzowej.

UWAGA:

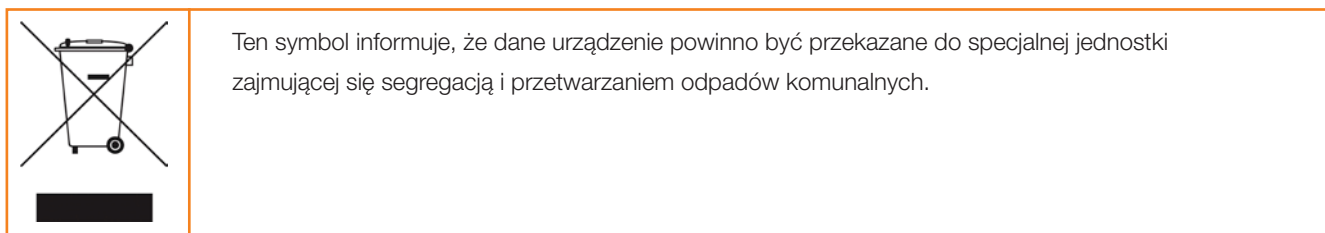
- Aby zniwelować ryzyko pożaru, używaj jedynie kabla telekomunikacyjnego nr 26 AWG lub grubszego.
- Zawsze odłączaj wszystkie linie telefoniczne z gniazdka przed naprawą lub rozbiórką urządzenia

OSTRZEŻENIE

- Odłącz zasilanie od urządzenia, zanim zaczniesz naprawę.
- Parametry zasilacza są podane w Załącznik B - Specyfikacje



Chroń nasze środowisko naturalne.



Pudełko kartonowe, plastik znajdujący się w opakowaniu, oraz części które są elementami routera mogą być segregowane w zgodzie z miejscowymi regulacjami prawnymi. Nigdy nie wyrzucaj tego urządzenia elektronicznego razem z odpadkami z Twojego gospodarstwa domowego. Możesz w związku z tym zostać pociągnięty do odpowiedzialności karnej lub innej przez lokalne organy ścigania. Proszę postępuj odpowiedzialnie i zdobądź informacje o wyrzuceniu urządzenia od lokalnej jednostki samorządowej.

Spis treści

| | |
|--|----|
| Rozdział 1. Wstęp | 6 |
| 1.1 Właściwości urządzenia | 6 |
| 1.2 Zastosowanie | 6 |
| Rozdział 2. Instalacja | 7 |
| 2.1 Konfiguracja sprzętu | 7 |
| 2.2 Panel przedni - diody informacyjne LED | 9 |
| Rozdział 3. Interfejs użytkownika WWW | 10 |
| 3.1 Ustawienia domyślne | 10 |
| 3.2 Konfiguracja IP | 11 |
| 3.3 Logowanie | 13 |
| Rozdział 4. Informacje o urządzeniu | 16 |
| 4.1 Statystyki | 16 |
| 4.1.1 Statystyki LAN | 16 |
| 4.1.2 Statystyki WAN | 16 |
| 4.1.3 Statystyki xTM | 17 |
| 4.1.4 Statystyki xDSL | 18 |
| 4.2 Routing | 22 |
| 4.3 ARP | 22 |
| 4.4 DHCP | 23 |
| 4.5 Sesje NAT | 23 |
| Rozdział 5. Zaawansowana konfiguracja | 24 |
| 5.1 WAN | 24 |
| 5.2 LAN | 27 |
| 5.3 NAT | 28 |
| 5.3.1 Serwery wirtualne | 28 |
| 5.3.2 Wyzwalanie portów | 29 |
| 5.3.3 Host DMZ | 31 |
| 5.4 Bezpieczeństwo | 31 |
| 5.4.1 Filtrowanie adresów IP | 31 |
| 5.5 Kontrola rodzicielska | 33 |
| 5.5.1 Ograniczenia czasu dostępu | 33 |
| 5.5.2 Filtr URL | 34 |
| 5.6 UPnP | 35 |
| 5.7 DNS Proxy/Relay | 35 |
| 5.8 Serwer wydruku | 35 |
| 5.9 Zarządzanie energią | 36 |

| | |
|--|----|
| Rozdział 6. Sieć bezprzewodowa | 37 |
| 6.1 Podstawowa konfiguracja | 37 |
| 6.2 Bezpieczeństwo | 38 |
| 6.2.1 WPS | 41 |
| 6.3 Filtrowanie MAC | 45 |
| 6.4 Zaawansowana konfiguracja | 46 |
| 6.5 Informacje o urządzeniach | 48 |
| | |
| Rozdział 7. Połączenia głosowe | 49 |
| 7.1 Ustawienia Podstawowe SIP | 49 |
| 7.1.1 Parametry globalne | 50 |
| 7.1.2 Usługodawca | 51 |
| 7.2 Zaawansowane ustawienia SIP | 53 |
| 7.2.1 Parametry globalne | 53 |
| 7.2.2 Usługodawca | 55 |
| 7.3 Ustawienia Debugowania SIP | 57 |
| 7.3.1 Parametry globalne | 57 |
| 7.3.2 Usługodawca | 58 |
| 7.4 Połączenia telefoniczne | 58 |
| | |
| Rozdział 8. Diagnostyka | 61 |
| | |
| Rozdział 9. Zarządzanie | 62 |
| 9.1 Ustawienia | 62 |
| 9.1.1 Przywróć ustawienia domyślne | 62 |
| 9.2 Logi systemowe | 63 |
| 9.3 Zarządzanie kontem | 65 |
| 9.3.1 Hasła | 65 |
| 9.4 Ponowne uruchomienie | 66 |
| | |
| Załącznik A – Zapora sieciowa | 67 |
| Załącznik B - Specyfikacje | 69 |
| Załącznik C – Zewnętrzny Rejestrator WPS | 71 |
| Załącznik D – Serwer Wydruku | 74 |

Rozdział 1. Wstęp

Router VI-3223u Multi-DSL WLAN IAD pozwala na przewodowy i bezprzewodowy dostęp wysokiej przepustowości w domu lub biurze. Wyposażony jest w cztery porty Sieci lokalnej RJ-45, oraz wspiera ADSL2+ i VDSL2 przez port RJ-11. ADSL2+ wspiera wiele jednoczesnych połączeń internetowych, podczas gdy VDSL2 jest połączeniem odpowiednim dla usług triple-play (Wideo + Dźwięk + Dane).

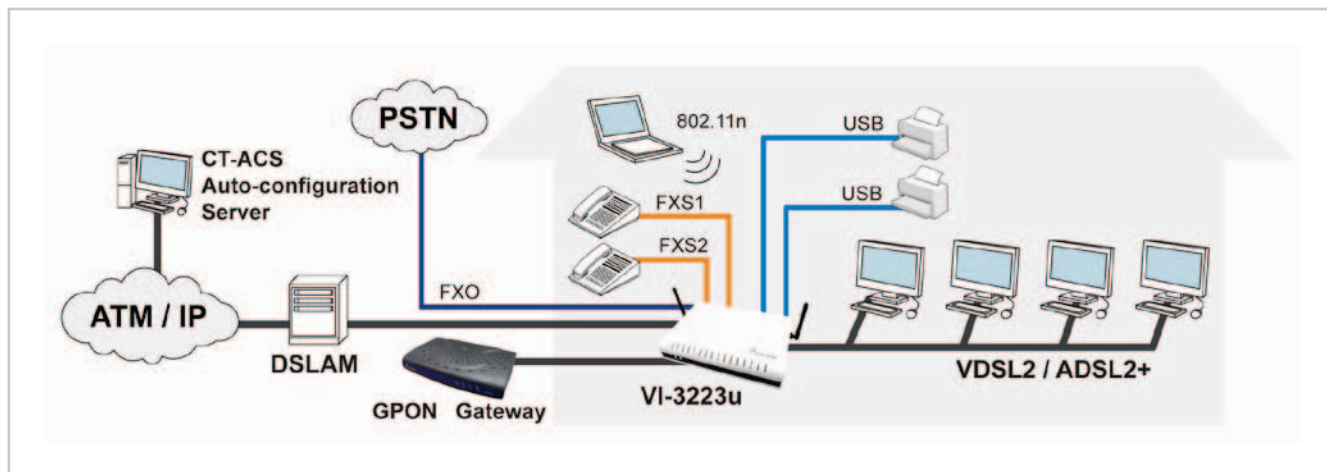
Zintegrowany punkt dostępowego WLAN ACCESS Point (AP) zgodny ze standardem 802.11n pozwala na szybszy dostęp bezprzewodowy ze zwiększonym zasięgiem, w porównaniu do 802.11b i 802.11g, oraz pozwala na wsteczną kompatybilność z tymi starszymi standardami. Przyciski WPS (Wi-Fi Protected Setup) oraz Wi-Fi On/Off znajdują się z przodu obudowy w celu łatwiejszego dostępu do funkcji obsługi sieci Wi-Fi.

1.1 Właściwości urządzenia

- Zintegrowany punkt dostępu 802.11n (kompatybilny z 802.11b/g)
- VI-3223u - Annex A
- Wsparcie dla profilu VDSL2 17a
- QoS na poziomie pakietów IP oraz per VC
- WAP and 802.1x
- Statyczny routing & RIP/RIP v2
- NAT/PAT
- IGMP Proxy
- Zarządzanie przez stronę WWW
- Automatyczne przełączanie pomiędzy ADSL2+ / VDSL2 zgodnie z ustawieniami DSLAM
- Wsparcie dla VPN Pass-Through
- Wsparcie dla T.38
- Automatyczna konfiguracja PVC
- IP/MAC filtrowanie
- Dynamiczne przypisywanie IP
- Kontrola rodzicielska
- DHCP Server/Relay/Client
- Wsparcie dla połączeń alarmowych
- Wsparcie dla wyświetlania i blokowanie numeru dzwoniącego
- Wsparcie dla bezpośrednie wybieranie numeru
- Wspiera zdalne zarządzanie

1.2 Zastosowanie

Następujący rysunek pokazuje typowe zastosowanie routera VI-3223u



Rozdział 2 Instalacja

2.1 Konfiguracja sprzętu

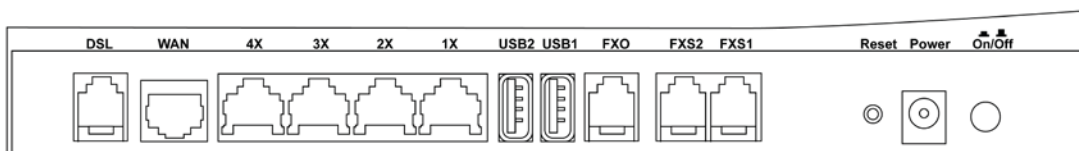
Postępuj zgodnie z instrukcją poniżej.



Nie stawiaj urządzeń na sobie! Te urządzenia nie mogą pracować ustawione jedno na drugim. Może to powodować pogorszenie osiągnięć, przegrzewanie się routera, a w efekcie jego uszkodzenie.

Panel Tylny

Poniższy rysunek pokazuje tylny panel urządzenia



Port DSL

Podłącz linię ADSL2+/VDSL do tego portu używając kabla telefonicznego (RJ-11).

Port WAN

Podłącz do źródła Internetu używając kabla RJ-45

Porty LAN

Użyj kabli RJ-45 klasy 1000-BASE-T aby podłączyć do czterech urządzeń do sieci Gigabit LAN lub 10/100BASE-T RJ-45 dla wolniejszych sieci. Porty automatycznie rozpoznają kable MDI/X typu prostego lub skrosowane.

Porty USB

Dwa porty USB 2.0 wspierają kompatybilne drukarki. Sprawdź Załącznik D w celu uzyskania instrukcji. Wsparcie dla innych urządzeń może być dodane w następujących aktualizacjach oprogramowania.

Port FXO

Jeśli chcesz podłączyć router i telefon do jednej linii, podłącz port FXO do splittera POTS za pomocą kabla RJ-11. Po odłączeniu zasilania podłącz port FXO do linii PSTN.

Porty FXS

Podłącz telefony kablem RJ-11, aby skorzystać z sieci VoIP.

Przycisk Reset

Przywróć ustawienia domyślne urządzenia wciskając przycisk Reset przez 5 do 10 sekund.

UWAGA: Jeśli przycisk zostanie wciśnięty przez powyżej 20 sekund router VI-3223u zostanie zablokowany (dioda Power świeci się na kolor czerwony). Przed resetem modemu należy skontaktować się z obsługą techniczną.

Power ON

Wciśnij przycisk, aby znalazł się w pozycji OFF (wyciśnięty). Podłącz zasilacz do gniazda zasilania w urządzeniu. Podłącz zasilacz do gniazdzka w ścianie lub do listwy zasilającej. Wciśnij przycisk Power, aby znalazł się w pozycji ON (wciśnięty). Jeśli wskazania LED są poprawne, urządzenie jest gotowe do konfiguracji (sprawdź rozdział 2.2 Panel przedni - diody informacyjne LED).

UWAGA 1: Jeśli urządzenie nie włącza się lub nie działa, sprawdź czy wszystkie kable zasilające są podłączone prawidłowo i uruchom ponownie urządzenie. Jeśli problem nadal występuje skontaktuj się ze wsparciem technicznym.

UWAGA 2: Przed naprawą lub rozebraniem urządzenia, odłącz wszystkie przewody zasilające oraz telefoniczne od urządzenia.

Panel Przedni

Przyciski WiFi & WPS znajdują się z lewej strony panelu, zgodnie z rysunkiem.



Przycisk Wi-Fi

Wciśnij ten przycisk, aby włączyć sieć Wi-Fi

Przycisk WPS

Wciśnij ten przycisk aby rozpocząć wyszukiwanie klientów WPS. Klienci ci muszą również wspierać tryb WPS. Jeśli WPS jest aktywny, Dioda LED WPS będzie się świeciła.

2.2 Panel przedni – diody informacyjne LED

Diody informacyjne LED panelu przedniego są pokazane i wyjaśnione poniżej. Informacje te może być wykorzystana do sprawdzenia stanu urządzenia i jego połączeń.



| LED | Kolor | Tryb | Funkcja |
|-----------|--------------|------|--|
| POWER | Zielony | | Wł. Urządzenie jest włączone. |
| | | | Wył. Urządzenie jest wyłączone. |
| | Czerwony | | Wł. Błąd POST (Power On Self Test): może być to dowolny błąd wewnętrznej sekwencji uruchamiania urządzenia lub stan w którym niemożliwe jest podłączenie do sieci i przesyłania danych użytkownika. |
| | Pomarańczowy | | Wł. Jeśli przycisk Reset był wciśnięty przez więcej niż 5 sekund, w celu przywrócenia ustawień fabrycznych, dioda zasilania powinna zmienić kolor na pomarańczowy (migać przez 1 sekundę) powiadamiając o gotowości do restartu fabrycznego. |
| LAN 1X-4X | Zielony | | Wł. Ustanowiono połączenie sieci lokalnej. |
| | | | Wył. Brak połączenia sieci lokalnej. |
| | | | Miga. Transmisja danych w sieci lokalnej. |
| WAN | Czerwony | | Wł. Ustanowiono połączenie sieci lokalnej WAN z prędkością 1000 Mb/s. |
| | | | Wył. Brak połączenia sieci lokalnej WAN. |
| | | | Miga. Transmisja danych po interfejsie WAN |
| | Zielony | | Wł. Ustanowiono połączenie sieci lokalnej WAN z prędkością 10/100 Mb/s. |
| | | | Wył. Brak połączenia sieci lokalnej WAN. |
| | | | Miga. Transmisja danych w sieci lokalnej WAN. |
| WLAN | Zielony | | Wł. Moduł bezprzewodowy jest gotowy (zainstalowany i uruchomiony). |
| | | | Wył. Moduł bezprzewodowy jest nieaktywny (nie jest zainstalowany lub uruchomiony). |
| | | | Miga. Transmisja danych w sieci WLAN. |
| WPS | Zielony | | Wł. WPS jest aktywny i urządzenie PC jest połączone do sieci WLAN. |
| | | | Wył. WPS wyłączony (wyłącza się po 5 minutach). |
| | | | Miga. Router szuka klientów WPS lub WPS nie jest skonfigurowany. |
| FXS / FXO | Zielony | | Wł. FXS telefon / FXO ma podniesioną słuchawkę. |
| | | | Wył. Telefon FXS / FXO ma odłożoną słuchawkę. |
| DSL | Zielony | | Wł. Ustanowiono połączenie DSL. |
| | | | Wył. Brak połączenia DSL. |
| | | | Miga. Testowanie połączenia DSL. |
| INTERNET | Zielony | | Wł. Sieć IP połączona, brak transmisji danych, Jeśli sesja IP lub PPPoE została odłączona, powiadomienie nadal pozostanie zielone, jeśli sesja ADSL jest aktywna. |
| | | | Wył. Modem wyłączony, w trybie mostka lub brak połączenia ADSL, dodatkowo, jeśli sesja IP lub PPPoE jest zerwana z innego powodu niż nieaktywność powiadomienie jest wyłączone. |
| | | | Miga. Połączenie IP aktywne, oraz ruch IP przesyłany przez urządzenie. |
| | Czerwony | | Wł. Urządzenie nie uzyskało połączenia IP (brak odpowiedzi DHCP, brak PPPoE lub brak uwierzytelnienia PPPoE, brak odpowiedzi adresu IP z IPCP, itd). |

Rozdział 3. Interfejs użytkownika WWW

Ten rozdział opisuje jak uzyskać dostęp do urządzenia przez interfejs WWW używając przeglądarki internetowej, takiej jak Internet Explorer (wersja 5.0 lub późniejsza).

3.1 Ustawienia domyślne

Ustawienia fabryczne urządzenia są wymienione poniżej:

- Adres IP LAN: 10.0.0.1
- Maska podsieci LAN: 255.255.255.0
- Dostęp dla użytkownika (użytkownik: user, hasło: user)

UWAGA: W trakcie pierwszej konfiguracji zalecane jest zmiana domyślnego hasła dostępu do routera. Należy to wykonać w zakładce Zarządzanie, następnie przejść do Zarządzanie kontem, i wybrać Hasła. (sprawdź rozdział 9.3.1 Hasła)

Informacja techniczna

Podczas uruchamiania urządzenia, wszystkie ustawienia są przywracane do wartości domyślnych. Następnie odczytany zostanie profil konfiguracji z pamięci lub pamięci flash. Wartości domyślne są nadpisane nowymi wartościami, jeśli zostały odpowiednio wcześniej skonfigurowane. Konfiguracja w pamięci może zostać utworzona przez interfejs WWW. Konfiguracja fabryczna może zostać przywrócona przez wciśnięcie przycisku reset przez 5 sekund, aż dioda LED zasilania będzie migać.

UWAGA: Jeśli przycisk zostanie wciśnięty przez powyżej 20 sekund router VI-3223u zostanie zablokowany (dioda Power świeci się na kolor czerwony). Przed resetem modemu należy skontaktować się z obsługą techniczną.

3.2 Konfiguracja IP

Tryb DHCP

Podczas uruchamiania routera VI-3223u aktywowany jest na nim serwer DHCP. Jego rola to przydzielanie adresów IP urządzeniom sieci LAN, czyli twoim komputerom.

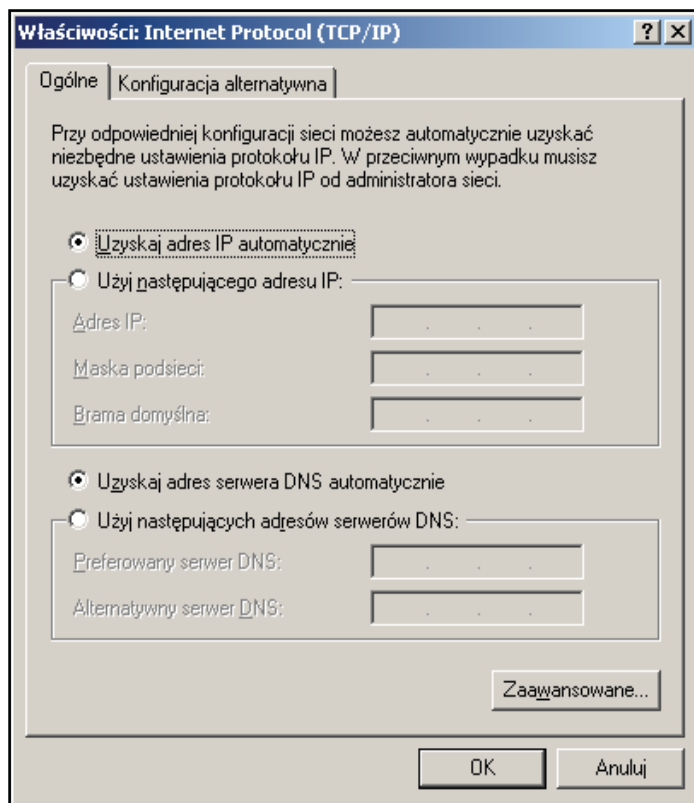
Aby uzyskać adres IP z serwera DHCP, postępuj wg kroków wymienionych poniżej.

UWAGA: Ta procedura zakłada, że używasz systemu Windows XP, aczkolwiek, główne kroki wymienione poniżej są zbliżone dla wszystkich systemów operacyjnych. Skorzystaj ze wsparcia dla twojego systemu, aby uzyskać dalsze informacje.

KROK 1: Z okna Połączeń sieciowych wybierz **Połączenie sieci lokalnej** (Local Area Connection). Możesz również uzyskać dostęp do tego okna przez dwukrotne kliknięcie ikony Połączenie sieci lokalnej na twoim pasku zadań. Kliknij przycisk **Właściwości**.

KROK 2: Wybierz **Internet Protocol (TCP/IP)** oraz kliknij przycisk **Właściwości**.

KROK 3: Wybierz opcję **“Uzyskaj adres IP automatycznie”**.



KROK 4: Wybierz **OK**, aby zapisać ustawienia.

Jeśli masz problem z połączeniem DHCP, spróbuj trybu IP statycznego.

Tryb IP statycznego

W trybie statycznego adresu IP, podajesz adresy komputerów samodzielnie.

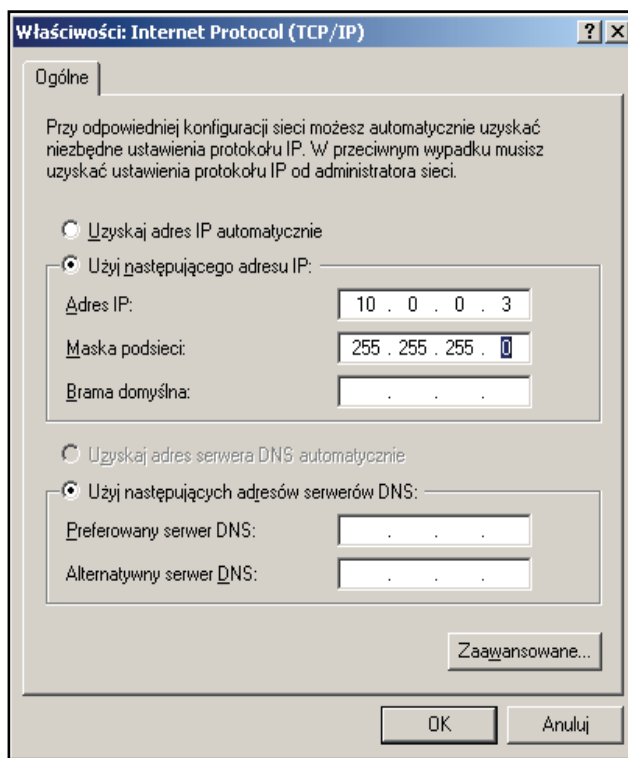
Postępuj według poniższych kroków, aby skonfigurować adres z podsieci 10.0.0.x, ustawionej domyślnie na modemie lub by skorzystać z adresacji publicznej.

UWAGA: Ta procedura zakłada, że używasz systemu Windows XP, aczkolwiek, główne kroki wymienione poniżej są zbliżone dla wszystkich systemów operacyjnych. Skorzystaj ze wsparcia dla twojego systemu, aby uzyskać dalsze informacje.

KROK 1: Z okna Połączeń sieciowych wybierz **Połączenie sieci lokalnej** (Local Area Connection). Możesz również uzyskać dostęp do tego okna przez dwukrotne kliknięcie ikony Połączenie sieci lokalnej na twoim pasku zadań. Kliknij przycisk **Właściwości**.

KROK 2: Wybierz **Internet Protocol (TCP/IP)** oraz kliknij przycisk **Właściwości**.

KROK 3: Wybierz opcję **Użyj następującego adresu IP**. Zmień adres IP na jeden z podsieci 10.0.0.x ($1 < x < 255$) z maską podsieci 255.255.255.0. Ekran powinien wyglądać jak poniżej:



KROK 4: Wybierz **OK** aby zapisać ustawienia.

3.3 Logowanie

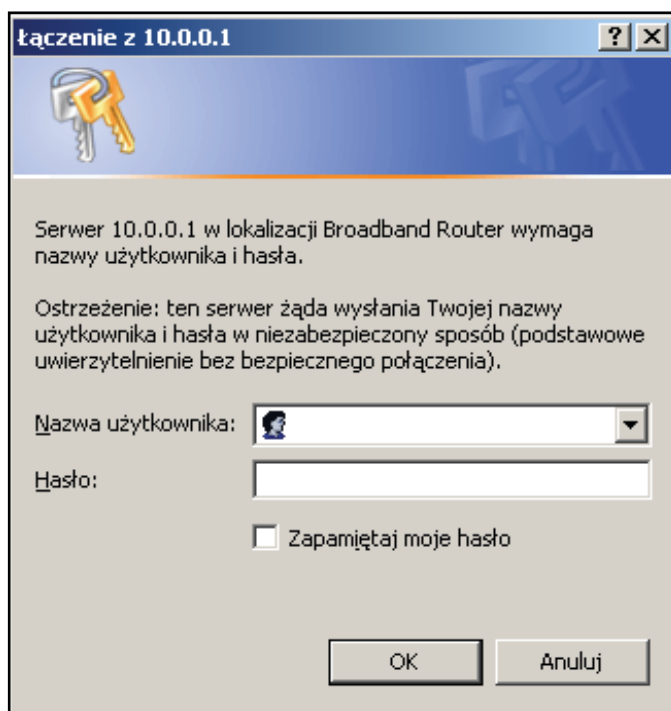
Postępuj wg poniższych instrukcji, aby uzyskać dostęp do konfiguracji routera za pomocą strony WWW

UWAGA: Ustawienia domyślne znajdują się w rozdziale 3.1 Ustawienia domyślne

KROK 1: Uruchom przeglądarkę internetową i wpisz adres IP routera. Jeśli jest niezmieniony, to domyślny adres to 10.0.0.1. W polu adresu wpisz zatem adres: http://10.0.0.1

UWAGA: W celu zarządzania siecią lokalną komputer z przeglądarką musi być podłączony do sieci lokalnej, niekoniecznie do samego urządzenia.

KROK 2: Pokaże się okno dialogowe, jak na rysunku poniżej, wpisz nazwę użytkownika i hasło (domyślne wartości znajdują się w rozdziale 3.1 Ustawienia domyślne).




KROK 3: Wybierz OK aby kontynuować.

UWAGA: Hasło może zostać zmienione (sprawdź rozdział 9.3.1 Hasła).

KROK 4: Po prawidłowym zalogowaniu, zobaczysz ten ekran:

File Edit View History Bookmarks Tools Help

najlepszy biznesowy internet



Informacja o urządzeniu

- Zaawansowana konfiguracja
- Bezprzewodowy
- Połączenie głosowe
- Diagnostyka
- Zarządzanie
- Język
- użytkownik: root

Informacja o urządzeniu

| | |
|-----------------------------|---------------------------------------|
| Numer wersji sprzętowej | 96368MIT-1341 N |
| Wersja oprogramowania | M631-S410TPS-T01_R09.A2pv6C035j1.d23e |
| Wersja bootloader (CPE) | 1.0.37-110.4-1 |
| DSL PHY i wersja sterownika | A2pv6C035j1.d23e |
| Wersja sterownika Wireless | 5.100.123.0.cpe4.10L02.6 |
| Numer seryjny | 0 |
| Adres MAC | 38:72:c0:98:55:00 |

Ta informacja odzwierciedla aktualny status połączenia WAN.

| | |
|------------------------------------|-------------------------|
| Szybkość linii - Wysyłanie (Kbps) | 0 |
| Szybkość linii - Odbieranie (Kbps) | 0 |
| Adres IPv4 LAN | 10.0.0.1 |
| Domyślna brama | eth0.1 |
| Preferowany serwer DNS | 10.255.253.249 |
| Alternatywny serwer DNS | 0.0.0.0 |
| Adres IPv6 LAN | |
| Domyślna brama IPv6 | |
| Data/Godzina | Thu Jan 1 01:44:03 1970 |

Informacja ta odzwierciedla stan rejestracji połączenia VoIP.

| | |
|-------------------------------|----------|
| telefon 0_0 Stan Rejestracja: | Disabled |
| telefon 0_1 Stan Rejestracja: | Disabled |

[Odśwież](#)

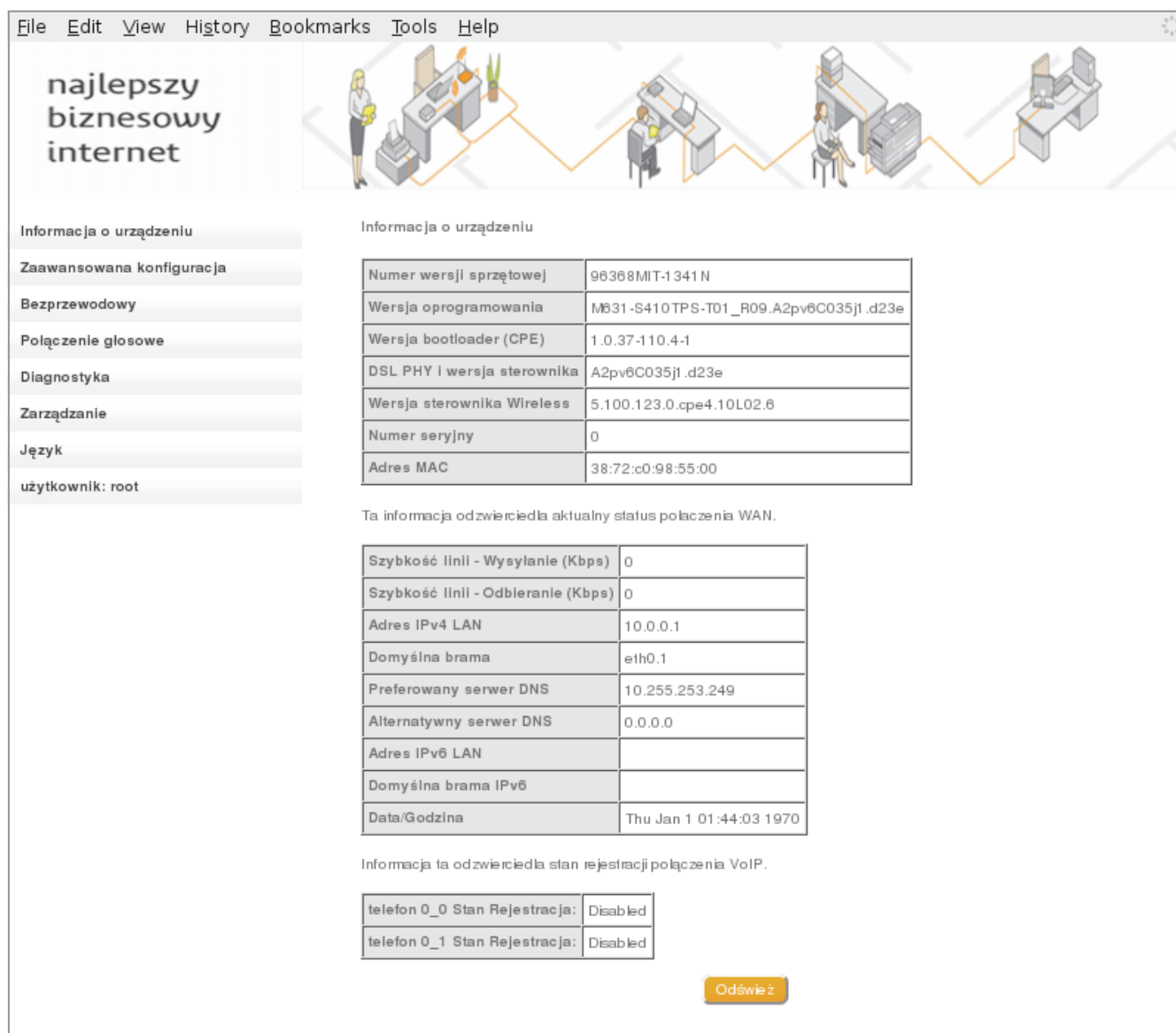
Rozdział 4. Informacje o urządzeniu

Interfejs WWW użytkownika jest podzielony na dwie ramki. Główne menu (po lewej) i ekran wyświetlający informacje (po prawej). Główne menu zawiera wiele opcji, a wybranie dowolnej z nich otwiera menu niższego poziomu z większą ilością opcji.

UWAGA: Pozycje menu pokazane poniżej zależą od skonfigurowanych połączeń, ustawień użytkownika, oraz jego uprawnień. Na przykład jeśli ustawienia NAT oraz Firewall są aktywne, główne menu wyświetli ustawienia NAT i bezpieczeństwa. Jeśli jedno z nich jest nieaktywne, dane menu również będzie nieaktywne.

Informacje o urządzeniu to pierwsza sekcja głównego menu, dlatego będzie opisana jako pierwsza. Kolejne rozdziały będą opisywać następane opcje menu w kolejności ich występowania.

Ekran Informacji o urządzeniu uruchamia się po zalogowaniu.



The screenshot shows a web browser interface with a menu on the left and a main content area on the right. The menu includes options like 'Informacja o urządzeniu', 'Zaawansowana konfiguracja', 'Bezprzewodowy', 'Połączenie głosowe', 'Diagnostyka', 'Zarządzanie', 'Język', and 'użytkownik: root'. The main content area displays 'Informacja o urządzeniu' with a table of device details, a WAN connection status table, and a VoIP registration status table. A 'Odśwież' button is located at the bottom right of the main content area.

| Informacja o urządzeniu | |
|-----------------------------|---------------------------------------|
| Numer wersji sprzętowej | 96368MIT-1341N |
| Wersja oprogramowania | M631-S410TPS-T01_R09.A2pv6C035jl.d23e |
| Wersja bootloader (CPE) | 1.0.37-110.4-1 |
| DSL PHY i wersja sterownika | A2pv6C035jl.d23e |
| Wersja sterownika Wireless | 5.100.123.0.cpe4.10L02.6 |
| Numer seryjny | 0 |
| Adres MAC | 38:72:c0:98:55:00 |

Ta informacja odzwierciedla aktualny status połączenia WAN.

| | |
|------------------------------------|-------------------------|
| Szybkość linii - Wysyłanie (Kbps) | 0 |
| Szybkość linii - Odbieranie (Kbps) | 0 |
| Adres IPv4 LAN | 10.0.0.1 |
| Domyślna brama | eth0.1 |
| Preferowany serwer DNS | 10.255.253.249 |
| Alternatywny serwer DNS | 0.0.0.0 |
| Adres IPv6 LAN | |
| Domyślna brama IPv6 | |
| Data/Godzina | Thu Jan 1 01:44:03 1970 |

Informacja ta odzwierciedla stan rejestracji połączenia VoIP.

| | |
|-------------------------------|----------|
| telefon 0_0 Stan Rejestracja: | Disabled |
| telefon 0_1 Stan Rejestracja: | Disabled |

[Odśwież](#)

Ten ekran pokazuje informacje o ustawieniach urządzenia, oprogramowaniu, sieci IP oraz inne przydatne informacje.

4.1 Statystyki

Ten ekran pokazuje statystyki LAN, WAN, ATM/PTM i xDSL.

UWAGA: Informacje są odświeżane automatycznie co 15 sekund. Wciśnij przycisk Zresetuj statystyki, aby odświeżyć manualnie.

4.1.1 Statystyki LAN

Ten ekran pokazuje statystyki ruchu IP dla interfejsów LAN

Informacja o urządzeniu

Podsumowanie

WAN

Statystyki

Route

ARP

DHCP

sesji NAT

Statystyki LAN

| Interfejs | Odebrane | | | | Wysłane | | | |
|-----------|----------|---------|-------|----------|-----------|---------|-------|----------|
| | Bajty | Pakiety | Błędy | Zgubione | Bajty | Pakiety | Błędy | Zgubione |
| 1X | 32665039 | 78591 | 3 | 0 | 154778896 | 121628 | 0 | 0 |
| 2X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| wi0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Zresetuj statystyki
Odśwież

| Nagłówek | | Opis |
|-------------------|------------|----------------------------|
| Interfejs | | Numer interfejsu LAN |
| Odebrane/Wysłane: | - Bajty | Liczba Bajtów |
| | - Pakiety | Liczba pakietów |
| | - Błędy | Liczba pakietów z błędami |
| | - Zgubione | Liczba zgubionych pakietów |

4.1.2 Statystyki WAN

Ten ekran pokazuje statystyki każdego interfejsu WAN.

Podsumowanie

WAN

Statystyki

LAN

Usługa WAN

xTM

xDSL

Route

ARP

DHCP

| Interfejs | Opis | Odebrane | | | | Wysłane | | | |
|-----------|----------------|-----------|---------|-------|----------|-----------|---------|-------|----------|
| | | Bajty | Pakiety | Błędy | Zgubione | Bajty | Pakiety | Błędy | Zgubione |
| ppp0a0 | ppp0a_0_0_35 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ppp1.1 | pppoe_0_0_1.35 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth0.1 | eth | 426314626 | 356947 | 0 | 0 | 534958529 | 447695 | 0 | 0 |

Zresetuj statystyki
Odśwież

| | | |
|-------------------|----------------------|----------------------------|
| Nagłówek | Opis | |
| Interfejs | Numer interfejsu WAN | |
| Opis | Nazwa usługi WAN | |
| Odebrane/Wysłane: | - Bajty | Liczba Bajtów |
| | - Pakiety | Liczba pakietów |
| | - Błędy | Liczba pakietów z błędami |
| | - Zgubione | Liczba zgubionych pakietów |

4.1.3 Statystyki xTM

Następujący rysunek pokazuje statystyki Asynchronous Transfer Mode (xTM).

| Informacja o urządzeniu | | Statystyki interfejsu | | | | | | | | | | |
|-------------------------|--|---|------------------|------------------|-------------------|-------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------------------------|----------------------------|
| Podsumowanie | | Numer portu | Oktety wejściowe | Oktety wyjściowe | Pakiety wejściowe | Pakiety wyjściowe | Wejściowe komórki OAM | Wyjściowe komórki OAM | Wejściowe komórki ASM | Wyjściowe komórki ASM | Błędy wejściowych pakietów | Błędy wyjściowych pakietów |
| WAN | | <div style="text-align: center;"> Resetuj Odśwież </div> | | | | | | | | | | |
| Statystyki | | | | | | | | | | | | |
| LAN | | | | | | | | | | | | |
| Usługa WAN | | | | | | | | | | | | |
| xTM | | | | | | | | | | | | |
| xDSL | | | | | | | | | | | | |
| Route | | | | | | | | | | | | |
| ARP | | | | | | | | | | | | |
| DHCP | | | | | | | | | | | | |

| | |
|----------------------------|---|
| Nagłówek | Opis |
| Numer portu | PORT ATM (0-3) |
| Oktety wejściowe | Liczba oktetów odebranych przez interfejs |
| Oktety wyjściowe | Liczba oktetów wysłanych przez interfejs |
| Pakiety wejściowe | Liczba pakietów odebranych przez interfejs |
| Pakiety wyjściowe | Liczba pakietów wysłanych przez interfejs |
| Wejściowe komórki OAM | Liczba komórek OAM odebranych przez interfejs |
| Wyjściowe komórki OAM | Liczba komórek OAM wysłanych przez interfejs |
| Wejściowe komórki ASM | Liczba komórek ASM odebranych przez interfejs |
| Wyjściowe komórki ASM | Liczba komórek ASM wysłanych przez interfejs |
| Błędy pakietów wyjściowych | Liczba błędów wyjściowych |
| Błędy pakietów wejściowych | Liczba błędów wejściowych |

4.1.4 Statystyki xDSL

Ten ekran pokazuje statystyki na interfejsie xDSL.

| | |
|--------------------------------|------------------------|
| Informacja o urządzeniu | Statystyki xDSL |
| Podsumowanie | |
| WAN | |
| Statystyki | |
| LAN | |
| Usługa WAN | |
| xTM | |
| xDSL | |
| Route | |
| ARP | |
| DHCP | |
| sesji NAT | |
| Zaawansowana konfiguracja | |
| Bezprzewodowy | |
| Połączenie głosowe | |
| Diagnostyka | |
| Zarządzanie | |
| Język | |
| użytkownik: root | |

| | | |
|---|----------------------------|---------------------------|
| Tryb: | | |
| Typ ruchu: | | |
| Status: | | Wyłączony |
| Stan zasilania łącza: | | |
| | | |
| | Szybkość odbierania | Szybkość wysyłania |
| Kodowanie liniowe (Trellis): | | |
| SNR stosunek sygnału do szumu (0.1 dB): | | |
| Oslabienie (0.1 dB) | | |
| Moc wyjściowa (0.1 dBm) | | |
| Osiągalna szybkość (Kbps): | | |
| Szybkość (Kbps): | | |
| | | |
| Super ramki: | | |
| Błędy super ramki: | | |
| Słowa RS: | | |
| Możliwe do skorygowania błędy RS | | |
| Niemożliwe do skorygowania błędy RS | | |
| | | |
| Błędy HEC: | | |
| Błędy OCD: | | |
| Błędy LCD: | | |
| Wszystkie komórki: | | |
| Komórki danych: | | |
| Błędne bity: | | |
| | | |
| Wszystkie ES: | | |
| Wszystkie SES: | | |
| Wszystkie UAS: | | |

TEST xDSL BER **Zresetuj statystyki**

Odśwież Statystyki

Przykład ADSL jest pokazany poniżej

Device Info

Summary

WAN

Statistics

LAN

WAN Service

xTM

xDSL

Route

ARP

DHCP

NAT Session

Advanced Setup

Wireless

Voice

Diagnostics

Management

Language

Statistics -- xDSL

| | | | | |
|--|-------------------|-----------------|-------------------|-----------------|
| Mode: | ADSL_G.dmt | | | |
| Traffic Type: | ATM | | | |
| Status: | Up | | | |
| Link Power State: | LO | | | |
| | Downstream | Upstream | | |
| Line Coding(Trellis): | Off | Off | | |
| SNR Margin (0.1 dB): | 166 | 120 | | |
| Attenuation (0.1 dB): | 5 | 140 | | |
| Output Power (0.1 dBm): | 191 | 46 | | |
| Attainable Rate (Kbps): | 11512 | 916 | | |
| | Path 0 | | Path 1 | |
| | Downstream | Upstream | Downstream | Upstream |
| Rate (Kbps): | 8032 | 640 | 0 | 0 |
| K (number of bytes in DMT frame): | 252 | 21 | 0 | 0 |
| R (number of check bytes in RS code word): | 0 | 16 | 0 | 0 |
| S (RS code word size in DMT frame): | 0.50 | 8.00 | 0.0 | 0.0 |
| D (interleaver depth): | 64 | 8 | 0 | 0 |
| Delay (msec): | 8.00 | 16.00 | 0.0 | 0.0 |
| INP (DMT symbol): | 0.00 | 0.22 | 0.0 | 0.0 |
| Super Frames: | 1415 | 1415 | 0 | 0 |
| Super Frame Errors: | 822 | 0 | 0 | 0 |
| RS Words: | 0 | 11517 | 0 | 0 |
| RS Correctable Errors: | 0 | 0 | 0 | 0 |
| RS Uncorrectable Errors: | 0 | 0 | 0 | 0 |
| HEC Errors: | 9176 | 0 | 0 | 0 |
| OCD Errors: | 0 | 0 | 0 | 0 |
| LCD Errors: | 0 | 0 | 0 | 0 |
| Total Cells: | 450951 | 0 | 0 | 0 |
| Data Cells: | 450951 | 0 | 0 | 0 |
| Bit Errors: | 0 | 0 | 0 | 0 |
| Total ES: | 14 | 0 | | |
| Total SES: | 14 | 0 | | |
| Total UAS: | 178 | 178 | | |

xDSL BER Test
Reset Statistics

Refresh

Wciśnij przycisk **Zresetuj statystyki** aby odświeżyć dane

| Pole | Opis |
|--|---|
| Tryb | G.Dmt, G.lite, T1.413, ADSL2, ADSL2+,VDSL, VDSL2 |
| Typ ruchu | Typ kanału Interleave lub Fast |
| Status | Pokazuje stan połączenia DSL |
| Stan zasilania łącza | Pokazuje stan zasilania łącza |
| Kodowanie liniowe (Trellis) | Trellis On/Off |
| SNR stosunek sygnału do szumu (0.1 dB) | Stosunek sygnału od szumu |
| Oslabienie (0.1 dB) | Wyliczenie średniego tłumienia linii w kierunku do urządzenia |
| Moc wyjściowa (0.1 dBm) | Całkowita moc w kierunku od urządzenia |
| Osiągalna szybkość (Kbps) | Maksymalna szybkość |
| Szybkość (Kbps) | Obecna szybkość |

W trybie VDSL, aktywna jest następująca sekcja.

| Pole | Opis |
|------------|--|
| B | Liczba bajtów w ramce danych MUX |
| M | Liczba ramek danych MUX w słowie kodowym RS. |
| T | Liczba ramek danych MUX w pod-ramce OH |
| R | Liczba bajtów redundantnych w słowie kodowym RS |
| S | Liczba symboli kodowych objętych słowem kodowym RS |
| L | Liczba bitów przesyłanych w każdym symbolu danych |
| D | Głębokość przeplotu |
| I | Rozmiar bloku przeplotu w bajtach |
| N | Rozmiar słowa kodowego RS |
| Opóźnienie | Opóźnienie w milisekundach (ms) |
| INP | Symbol DMT |

W trybie ADSL2+, aktywna jest następująca sekcja.

| Pole | Opis |
|------------|---|
| MSGc | Liczba bajtów w wiadomości nadmiarowej kanału |
| B | Liczba bajtów w ramce danych MUX |
| M | Liczba ramek danych MUX w ramce danych FEC |
| T | Ramki danych MUX nad bajtami synchronizacji |
| R | Liczba bajtów kontrolnych w ramce danych FEC |
| S | Stosunek długości ramek danych FEC do PMD |
| L | Liczba bitów ramki danych PMD |
| D | Głębokość przeplotu |
| Opóźnienie | Opóźnienie w milisekundach (ms) |
| INP | Symbol DMT |
| INP | Symbol DMT |

W trybie G.DMT, aktywna jest następująca sekcja

| Pole | Opis |
|--------------------------------------|--|
| K | Liczba bajtów w ramce DMT |
| R | Liczba bajtów kontrolnych w słowie kodowym RS |
| S | Rozmiar słowa kodowego RS w ramce DMT |
| D | Głębokość przeplotu |
| Opóźnienie | Opóźnienie w milisekundach (ms) |
| Ramki OH | Całkowita liczba ramek OH |
| Błędy ramek OH | Liczba ramek OH odebranych z błędami |
| Słowa RS | Liczba błędów kodowych Reeda-Solomona |
| Możliwe do skorygowania błędy RS | Liczba możliwych do skorygowania błędów RS |
| Nieemożliwe do skorygowania błędy RS | Liczba niemożliwych do skorygowania błędów RS |
| Błędy HEC | Liczba błędów sumy kontrolnej błędu nagłówka |
| Błędy OCD | Liczba błędów liniowości poza komórkami |
| Błędy LCD | Liczba błędów straty liniowości komórek |
| Wszystkie komórki | Liczba komórek ATM (komórki bezczynności oraz danych) |
| Komórki danych | Liczba komórek danych ATM |
| Błędne bity | Liczba błędnych bitów |
| Wszystkie ES | Liczba błędnych sekund (Errored Seconds) |
| Wszystkie SES | Liczba poważnie błędnych sekund (Severely Errored Seconds) |
| Wszystkie UAS | Liczba niedostępnych sekund (Unavailable Seconds) |

TEST xDSL BER

Kliknij na **Test xDSL BER** w oknie statystyk xDSL, aby sprawdzić stopę błędów (Bit Error Rate). Okno typu pop-up pokaże się na ekranie o wyglądzie jak poniżej.

ADSL BER Test - Start

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the test duration below and click "Start".

Tested Time (sec): ▼

Kliknij **Początek** aby zacząć lub kliknij **Zamknij**, aby anulować test.

Po zakończeniu testu, okno wyglądać będzie przykładowo tak:

ADSL BER Test - Result

The ADSL BER test completed successfully.

| | |
|--------------------------------|--------------------|
| Test Time (sec): | 20 |
| Total Transferred Bits: | 0x0000000000000000 |
| Total Error Bits: | 0x0000000000000000 |
| Error Ratio: | Not Applicable |

4.2 Routing

Wybierz menu **Routing** aby wyświetlić ścieżki IP odnalezione przez router.

| Informacja o urządzeniu | Informacje o urządzeniu - Routing | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------------------|---|----------------|-------|----------------|--------|-----------|--------|-----------|----------|---------|---------------|---|---|--|-----|--------------|---------|---------------|---|---|-----|--------|---------|----------------|---------|----|---|-----|--------|
| Podsumowanie | Flagi: U-podniesiona, I-odrzucona, G-brama, H-host, R-przywrócona D-dynamiczna (przekierowana), M-zmodyfikowana (przekierowana) | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| WAN | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Statystyki | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Route | <table border="1"> <thead> <tr> <th>Adres docelowy</th> <th>Brama</th> <th>Maska podsieci</th> <th>Flaga</th> <th>Metryka</th> <th>Usługa</th> <th>Interfejs</th> </tr> </thead> <tbody> <tr> <td>10.0.0.0</td> <td>0.0.0.0</td> <td>255.255.255.0</td> <td>U</td> <td>0</td> <td></td> <td>br0</td> </tr> <tr> <td>10.255.253.0</td> <td>0.0.0.0</td> <td>255.255.255.0</td> <td>U</td> <td>0</td> <td>eth</td> <td>eth0.1</td> </tr> <tr> <td>0.0.0.0</td> <td>10.255.253.254</td> <td>0.0.0.0</td> <td>UG</td> <td>0</td> <td>eth</td> <td>eth0.1</td> </tr> </tbody> </table> | Adres docelowy | Brama | Maska podsieci | Flaga | Metryka | Usługa | Interfejs | 10.0.0.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | | br0 | 10.255.253.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | eth | eth0.1 | 0.0.0.0 | 10.255.253.254 | 0.0.0.0 | UG | 0 | eth | eth0.1 |
| Adres docelowy | Brama | Maska podsieci | Flaga | Metryka | Usługa | Interfejs | | | | | | | | | | | | | | | | | | | | | | | |
| 10.0.0.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | | br0 | | | | | | | | | | | | | | | | | | | | | | | |
| 10.255.253.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | eth | eth0.1 | | | | | | | | | | | | | | | | | | | | | | | |
| 0.0.0.0 | 10.255.253.254 | 0.0.0.0 | UG | 0 | eth | eth0.1 | | | | | | | | | | | | | | | | | | | | | | | |
| ARP | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DHCP | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| sesji NAT | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Zaawansowana konfiguracja | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Bezprzewodowy | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| Pole | Opis |
|----------------|--|
| Adres docelowy | Docelowa podsieć lub host |
| Brama | Adres IP następnego punktu sieci |
| Maska podsieci | Maska podsieci docelowej |
| Flaga | U: Trasa aktywna |
| | !: Trasa odrzucona |
| | G: Użyj bramy |
| | H: Cel jest hostem |
| | R: Odtwórz trasę na potrzeby routingu dynamicznego |
| | D: Zainstalowana automatycznie przez demona M: Zmodyfikowana od trasy demona routingu |
| Metryka | Odległość do celu zazwyczaj mierzona w 'skokach'. Nie jest używana przez nowsze jądra, ale może być używana przez demony routingu. |
| Usługa | Pokazuje nazwę połączenia WAN |
| Interfejs | Pokazuje interfejs połączenia |

4.3 ARP

Wybierz **ARP**, aby pokazać ustawienia ARP.

| Informacja o urządzeniu | Informacje o urządzeniu - ARP | | | | | | | | | | | | | | | | |
|-------------------------|---|-------------------|------------|----------|------------|-----------|-----------|-------------------|-----|----------------|--------------|-------------------|--------|----------------|-----------|-------------------|--------|
| Podsumowanie | | | | | | | | | | | | | | | | | |
| WAN | | | | | | | | | | | | | | | | | |
| Statystyki | | | | | | | | | | | | | | | | | |
| Route | | | | | | | | | | | | | | | | | |
| ARP | <table border="1"> <thead> <tr> <th>Adres IP</th> <th>Flagi</th> <th>Adres HW</th> <th>Urządzenie</th> </tr> </thead> <tbody> <tr> <td>10.0.0.65</td> <td>Kompletny</td> <td>f0:4d:a2:22:c8:38</td> <td>br0</td> </tr> <tr> <td>10.255.253.178</td> <td>Niekompletny</td> <td>00:00:00:00:00:00</td> <td>eth0.1</td> </tr> <tr> <td>10.255.253.254</td> <td>Kompletny</td> <td>00:1b:d5:95:1e:dc</td> <td>eth0.1</td> </tr> </tbody> </table> | Adres IP | Flagi | Adres HW | Urządzenie | 10.0.0.65 | Kompletny | f0:4d:a2:22:c8:38 | br0 | 10.255.253.178 | Niekompletny | 00:00:00:00:00:00 | eth0.1 | 10.255.253.254 | Kompletny | 00:1b:d5:95:1e:dc | eth0.1 |
| Adres IP | Flagi | Adres HW | Urządzenie | | | | | | | | | | | | | | |
| 10.0.0.65 | Kompletny | f0:4d:a2:22:c8:38 | br0 | | | | | | | | | | | | | | |
| 10.255.253.178 | Niekompletny | 00:00:00:00:00:00 | eth0.1 | | | | | | | | | | | | | | |
| 10.255.253.254 | Kompletny | 00:1b:d5:95:1e:dc | eth0.1 | | | | | | | | | | | | | | |
| DHCP | | | | | | | | | | | | | | | | | |
| sesji NAT | | | | | | | | | | | | | | | | | |

| Pole | Opis |
|------------|---|
| Adres IP | Adres IP komputera |
| Flagi | Kompletny, niekompletny, stały, publikowany |
| Adres HW | Adres MAC komputera |
| Urządzenie | Interfejs połączenia |

4.4 DHCP

Wybierz **DHCP**, aby wyświetlić adresy przyznane przez serwer DHCP

Informacja o urządzeniu

- Podsumowanie
- WAN
- Statystyki
- Route
- ARP
- DHCP
- sesji NAT
- Zaawansowana konfiguracja
- Bezorzewodoww

Informacje o urządzeniu - dzierżawy DHCP

| Nazwa hosta | Adres MAC | Adres IP | Wygasa za |
|-----------------|-------------------|-----------|---------------------------------|
| OrangeLabs-LTE3 | 84:8f:69:ca:d7:50 | 10.0.0.64 | 2 hours, 43 minutes, 29 seconds |
| TP204474000003 | 00:50:da:bb:34:dd | 10.0.0.64 | 0 seconds |
| Komputer | f0:4d:a2:22:c8:38 | 10.0.0.65 | 56 seconds |
| TP204474000003 | 00:50:da:73:4f:c8 | 10.0.0.66 | 0 seconds |

[Odśwież Statystyki](#)

| Pole | Opis |
|-------------|--|
| Nazwa hosta | Pokazuje nazwę sieciową urządzenia |
| Adres MAC | Pokazuje adres MAC urządzenia |
| Adres IP | Pokazuje adres IP urządzenia |
| Wygasa za | Pokazuje ile czasu pozostało do zakończenia okresu, na jaki został przydzielony adres IP |

4.5 Sesje NAT

Sesje NAT są powiązaniem pomiędzy sesjami TCP w domenie lokalnej a sesjami TCP w domenie publicznej, poprzez mechanizm translacji NAT. Sesje NAT pozwala połączyć dwie reprezentacje sesji.

Informacja o urządzeniu

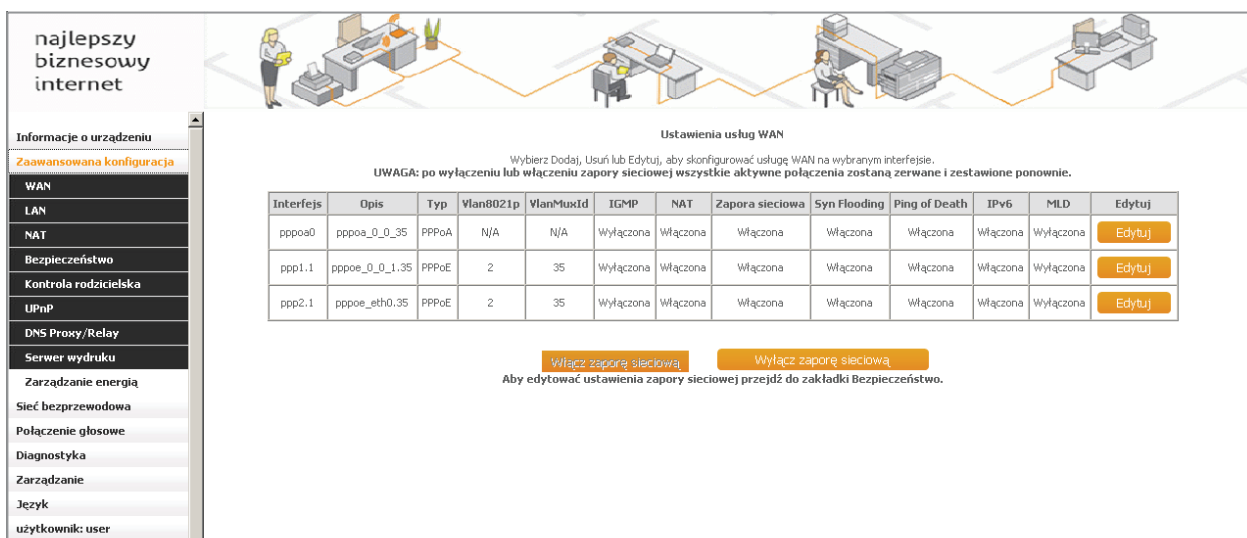
- Podsumowanie
- WAN
- Statystyki
- Route
- ARP
- DHCP
- sesji NAT
- Zaawansowana konfiguracja

sesji NAT

| IP Źródłowy | Port Źródłowy | IP docelowy | Port docelowy | Protokół | Limit czasu |
|-------------|---------------|-------------|---------------|----------|-------------|
| Refresh | | | | | |

Rozdział 5. Zaawansowana konfiguracja

5.1 WAN



Ten ekran pozwala na konfigurację interfejsów WAN jak również włączenie i wyłączenie firewala.

| Nagłówek | Opis |
|-----------------|--|
| Interfejs | Nazwa interfejsu WAN |
| Opis | Nazwa połączenia WAN |
| Typ | Typ połączenia |
| Vlan8021p | VLAN ID jest użyte do tagowania VLAN (IEEE 802.1Q) |
| VlanMuxId | Pokazuje VLAN ID 802.1Q |
| IGMP | Pokazuje stan (Internet Group Management Protocol) |
| NAT | Pokazuje stan NAT (Network Address Translation) |
| Zapora sieciowa | Pokazuje stan bezpieczeństwa |
| Syn Flooding | <p>Atak Syn flood, polega na wysyłaniu połączeń TCP szybciej, niż urządzenie jest je w stanie przetworzyć.</p> <ul style="list-style-type: none"> Atakujący tworzy losowy adres dla każdego pakietu. Flaga SYN w każdym pakiecie jest żądaniem otwarcia nowego połączenia do serwera z nieistniejącego adresu IP. Ofiara odpowiada na nieistniejący adres IP i czeka na potwierdzenie, które nigdy nie przychodzi (około 3 minuty). Tabela połączeń ofiary zapełnia się podczas oczekiwania. Po zapełnieniu tablicy, wszystkie nowe połączenia są ignorowane. Uprawnieni użytkownicy są również ignorowani i nie mogą uzyskać dostępu. Zazwyczaj serwer wraca do normalnego stanu w momencie przerwania ataku. Nowsze systemy operacyjne oferują lepsze zarządzanie zasobami, jest trudniej przepelnić w nich tablice, jednak wciąż mogą paść ofiarą ataku. <p>Atak Syn flood może być użyty jako część innych ataków, takich jak dezaktywacja jednej strony podczas przechwytywania połączenia TCP lub powstrzymanie uwierzytelnienia lub logowania pomiędzy serwerami.</p> |
| Ping of Death | Atak Ping of Death polega na wysyłaniu pakietów IP o rozmiarze większym niż 65,535 bajtów. Pakiety o tym rozmiarze są nieprawidłowe, ale możliwe jest stworzenie ich w specjalnej aplikacji. Prawidłowo napisane i zabezpieczone systemy operacyjne są w stanie wykryć takie pakiety, ale niektóre mogą paść ofiarą. Narzędzia typu ping ICMP zazwyczaj zawierają funkcjonalność wysyłania dużych pakietów, stąd nadały nazwę tej metodzie, choć UDP lub inne protokoły również mogą przekazywać Ping of Death. |
| IPv6 | Pokazuje adres IPv6 WAN |
| MLD | Pokazuje stan MLD (Multicast Listener Discovery) |
| Edytuj | Wybierz interfejs do edycji |

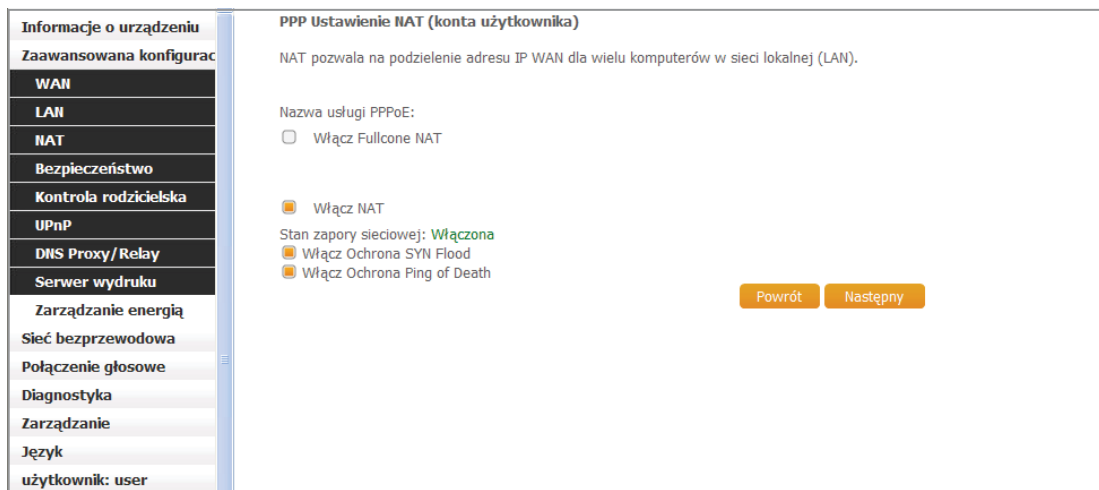
WŁĄCZ ZAPORĘ SIECIOWĄ

Kliknij przycisk Włącz zaporę sieciową by uruchomić firewall.

WYŁĄCZ ZAPORĘ SIECIOWĄ

Kliknij przycisk Wyłącz zaporę sieciową by wyłączyć firewall, jeśli funkcja Zapory sieciowej nie jest potrzebna.

Kliknij przycisk **Edytuj**, aby rekonfigurować połączenie.



WŁĄCZ FULLCONE NAT

Opcja jest dostępna jeśli włączana jest usługa NAT. Znana jako one-to-one NAT, wszystkie żądania z tego samego wewnętrznego adresu IP i portu są mapowane na taki sam zewnętrzny adres IP i port. Zewnętrzny host może wysłać pakiety do wewnętrznego hosta przez wysyłanie pakietów na zmapowany zewnętrzny adres.

WŁĄCZ NAT

Jeśli LAN został skonfigurowany z wykorzystaniem prywatnego adresu IP, użytkownik powinien zaznaczyć to pole wyboru. Po ponownym uruchomieniu w menu Zaawansowana konfiguracja pojawi się podmenu NAT. Jeśli prywatny adres IP nie został wykorzystany po stronie LAN (tzn. strona LAN wykorzystuje publiczny adres IP) to pole wyboru powinno pozostać niezaznaczone aby zwolnić zasoby systemowe i poprawić wydajność urządzenia.

WŁĄCZ OCHRONA SYN flood

– zaznacz to pole, aby włączyć ochronę przed atakami typu SYN flood.

WŁĄCZ OCHRONA Ping of Death

– zaznacz to pole, aby włączyć ochronę przed atakami typu Ping of Death.

Aby kontynuować kliknij przycisk **Następny** lub przycisk **Powrót** aby powrócić do poprzedniego ekranu.

Konfiguracja WAN - Podsumowanie

Upewnij się, że poniższe ustawienia są zgodne z ustawieniami podanymi przez usługodawcę internetowego.

| | |
|------------------------------|----------|
| Typ połączenia: | PPPoE |
| NAT: | Disabled |
| Full Cone NAT: | Disabled |
| Zapora sieciowa: | Disabled |
| Włącz Ochrona SYN Flood: | Disabled |
| Włącz Ochrona Ping of Death: | Disabled |
| Multiemisja IGMP: | Disabled |
| Jakość usług: | Disabled |

Kliknij przycisk "Zastosuj / Zapisz", aby ten interfejs był skuteczny. Kliknij "Wstecz" aby dokonać zmian.

[Powrót](#) [Zastosuj / Zapisz](#)

Ekran Konfiguracji WAN – Podsumowanie pokazuje szczegóły usługi WAN, którą właśnie skonfigurowano. Sprawdź wszystkie ustawienia a następnie kliknij przycisk **Zapisz/Zastosuj** jeśli są poprawne albo **Powrót** jeśli chcesz je poprawić.

Po kliknięciu przycisku **Zapisz/Zastosuj** na głównym ekranie powinna się pojawić nowa usługa. Aby ją aktywować musisz uruchomić ponownie router. Przejdź do Zarządzanie → Ponowne uruchomienie i kliknij przycisk **Uruchom ponownie**.

5.2 LAN

Skonfiguruj interfejs LAN, a następnie wciśnij **Zastosuj/Zapisz**.

Informacje o urządzeniu
Zaawansowana konfiguracja
WAN
LAN
NAT
Bezpieczeństwo
Kontrola rodzicielska
UPnP
DNS Proxy/Relay
Serwer wydruku
Zarządzanie energią
Sieć bezprzewodowa
Połączenie głosowe
Diagnostyka
Zarządzanie
Język
użytkownik: user

Ustawienia sieci lokalnej (LAN)
Skonfiguruj adres IP routera szerokopasmowego i maskę podsieci dla interfejsu LAN.

Adres IP:
Maska podsieci:

Stan zapory sieciowej: **Włączona**
 Wyłącz serwer DHCP
 Włącz serwer DHCP

Początkowy adres IP:
Końcowy adres IP:
Czas dzierżawy (godzina):

Włącz serwer DHCP Relay
DHCP Server IP Address:
Lista dzierżawy statycznego IP (maksymalnie 32 pozycje mogą zostać skonfigurowane)

| Adres MAC: | Adres IP: | Usuń |
|------------|-----------|--------------------------|
| | | <input type="checkbox"/> |

Sprawdź opis poszczególnych pól poniżej.

Adres IP: Wpisz adres IP portu LAN.

Maska podsieci: Wpisz maskę podsieci portu LAN.

Włącz serwer DHCP: Aby włączyć serwer DHCP, zaznacz przełącznik . Wpisz początkowy, końcowy adres IP i czas dzierżawy. Te ustawienia konfigurują router do automatycznego przydzielania adresów IP, domyślnej bramy, serwera DNS komputerom Twojej sieci LAN.

Włącz serwer DHCP Relay: Uruchom przełącznikiem oraz wpisz adres IP serwera DHCP. To pozwala routerowi na przekazywanie pakietów DHCP zdalnemu serwerowi DHCP. Zdalny serwer DHCP przypisze adres IP. Ta opcja jest ukryta, jeśli NAT jest aktywny lub gdy router jest skonfigurowany tylko w z jednym mostkowym PVC.

Lista dzierżawy statycznego IP: Maksymalnie 32 pozycje mogą być skonfigurowane.

| Adres MAC: | Adres IP: | Usuń |
|------------|-----------|------|
|------------|-----------|------|

Aby dodać wpis, wpisz adres MAC i statyczne IP, następnie kliknij **Zastosuj/Zapisz**.

| Adres MAC: | Adres IP: | Usuń |
|-------------------|-----------|-------------------------------------|
| 12:23:34:45:56:56 | 10.0.0.99 | <input checked="" type="checkbox"/> |

Aby usunąć pozycję, wybierz odpowiednie pole w kolumnie Usun i kliknij **Usuń wpisy**.

W tabelce poniżej znajdziesz opisy poszczególnych pól.

| Nagłówek | Opis |
|---|---|
| Użyj interfejsu | Wybierz interfejs WAN z listy. |
| Wybierz usługę lub Usługa niestandardowa | Wybierz usługę z listy lub Wpisz własną nazwę |
| Adres IP serwera | Wpisz adres IP serwera. |
| Początek portu zewnętrznego | Wpisz początkowy port zewnętrzny (jeśli wybierzesz standardową usługę zakres jest wybierany automatycznie). |
| Koniec portu zewnętrznego | Wpisz końcowy port zewnętrzny zakresu (jeśli wybierzesz standardową usługę zakres jest wybierany automatycznie). |
| Protokół | TCP, TCP/UDP lub UDP. |
| Początek portu wewnętrznego | Wpisz początkowy port wewnętrzny (gdy wpiszesz nazwę usługi niestandardowej). Gdy wybierzesz usługę z listy zakres jest konfigurowany automatycznie. |
| Koniec portu wewnętrznego | Wpisz końcowy port wewnętrzny (gdy wpiszesz nazwę usługi niestandardowej). Gdy wybierzesz usługę z listy zakres jest konfigurowany automatycznie. |

5.3.2 Wyzwalanie portów

Niektóre aplikacje wymagają otwarcia określonych portów w zaporze sieciowej routera dla uzyskania zdalnego dostępu. Wyzwalanie portów dynamicznie otwiera porty w zaporze, gdy aplikacja w sieci LAN zainicjuje połączenie TCP / UDP przy użyciu Wyzwalania portów router umożliwi zdalnej usłudze z sieci WAN ustanowienie nowych połączeń z powrotem do aplikacji po stronie sieci LAN za pomocą otwartych portów. Maksymalnie 32 wpisy mogą zostać skonfigurowane.

Informacja o urządzeniu

Zaawansowana konfiguracja

Interfejs Layer2

Usługa WAN

VPN

LAN

NAT

Serwery wirtualne

Wyzwalanie portów

Host DMZ

NAT - ustawienia wyzwalania portów

Niektóre aplikacje wymagają otwarcia określonych portów w zaporze sieciowej routera dla uzyskania zdalnego dostępu. Trigger Port dynamicznie otwiera porty w zaporze, gdy aplikacja w sieci LAN zainicjuje połączenie TCP / UDP przy użyciu "Triggering ports". Router umożliwia zdalnej usłudze z sieci WAN ustanowienie nowych połączeń z powrotem do aplikacji po stronie sieci LAN za pomocą "Otwartych portów". Maksymalnie 32 wpisy mogą zostać skonfigurowane.

Dodaj
Usuń

| Nazwa aplikacji | Trigger | | Otwarte | | Interfejs WAN | Usuń | | |
|-----------------|----------|---------------|---------|----------|---------------|------|---------------|--------|
| | Protokół | Zakres portów | | Protokół | | | Zakres portów | |
| | | Początek | Koniec | | | | Początek | Koniec |
| | | | | | | | | |

Aby dodać nową pozycję wybierz **Dodaj**. Pojawi się następujące okno.

Informacja o urządzeniu

Zaawansowana konfiguracja

Interfejs Layer2

Usługa WAN

VPN

LAN

NAT

Serwery wirtualne

Wyzwalanie portów

Host DMZ

Bezpieczeństwo

Kontrola rodzicielska

Jakość usługi

Routing

DNS

DSL

UPnP

DNS Proxy

Serwer wydruku

Grupowanie interfejsów

Tuneł IP

IPSec

NAT - ustawienia wyzwalania portów

Niektóre aplikacje wymagają otwarcia określonych portów w zaporze sieciowej routera dla uzyskania zdalnego dostępu. Trigger Port dynamicznie otwiera porty w zaporze, gdy aplikacja w sieci LAN zainicjuje połączenie TCP / UDP przy użyciu "Triggering ports". Router umożliwia zdalnej usłudze z sieci WAN ustanowienie nowych połączeń z powrotem do aplikacji po stronie sieci LAN za pomocą "Otwartych portów". Maksymalnie 32 wpisy mogą zostać skonfigurowane.
Porty (20, 21, 22, 23, 69, 80, 161, 443, 30005) są wykorzystywane przez ISP.
Pozostała liczba wpisów, które mogą zostać skonfigurowane:32

Użyj interfejsu:

Select an aplikacji:

Custom aplikacji:

Zastosuj / Zapisz

| Trigger portów Początek | Trigger portów Koniec | Trigger Protokół | Otwarte portów Początek | Otwarte portów Koniec | Otwarte Protokół |
|-------------------------|-----------------------|------------------|-------------------------|-----------------------|------------------|
| <input type="text"/> | <input type="text"/> | TCP ▼ | <input type="text"/> | <input type="text"/> | TCP ▼ |
| <input type="text"/> | <input type="text"/> | TCP ▼ | <input type="text"/> | <input type="text"/> | TCP ▼ |
| <input type="text"/> | <input type="text"/> | TCP ▼ | <input type="text"/> | <input type="text"/> | TCP ▼ |
| <input type="text"/> | <input type="text"/> | TCP ▼ | <input type="text"/> | <input type="text"/> | TCP ▼ |
| <input type="text"/> | <input type="text"/> | TCP ▼ | <input type="text"/> | <input type="text"/> | TCP ▼ |
| <input type="text"/> | <input type="text"/> | TCP ▼ | <input type="text"/> | <input type="text"/> | TCP ▼ |
| <input type="text"/> | <input type="text"/> | TCP ▼ | <input type="text"/> | <input type="text"/> | TCP ▼ |
| <input type="text"/> | <input type="text"/> | TCP ▼ | <input type="text"/> | <input type="text"/> | TCP ▼ |
| <input type="text"/> | <input type="text"/> | TCP ▼ | <input type="text"/> | <input type="text"/> | TCP ▼ |
| <input type="text"/> | <input type="text"/> | TCP ▼ | <input type="text"/> | <input type="text"/> | TCP ▼ |

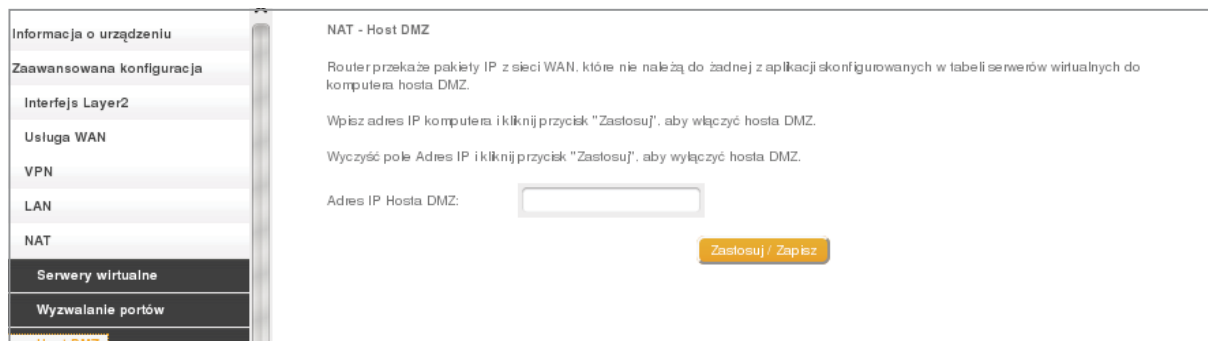
Zastosuj / Zapisz

W tabeli poniżej znajdziesz opisy poszczególnych pól.

| Nagłówek | Opis |
|--------------------------|--|
| Ubrać interfejsu | Wybierz interfejs WAN z listy |
| Wybierz aplikację | Wybierz aplikację z listy |
| Lub | Lub |
| Niestandardowa aplikacja | Wpisz swoją nazwę aplikacji |
| Trigger Portów Początek | Wpisz początkowy otwarty port (jeśli wybierzesz standardową usługę zakres jest wybierany automatycznie). |
| Trigger Portów Koniec | Wpisz końcowy otwarty port zakresu (jeśli wybierzesz standardową usługę zakres jest wybierany automatycznie). |
| Trigger Protokół | TCP, TCP/UDP lub UDP. |
| Otwarte porty początek | Wpisz początkowy port wyzwalania(gdy wpiszesz nazwę usługi niestandardowej). Gdy wybierzesz usługę z listy zakres jest konfigurowany automatycznie. |
| Otwarte porty koniec | Wpisz końcowy port wyzwalania(gdy wpiszesz nazwę usługi niestandardowej). Gdy wybierzesz usługę z listy zakres jest konfigurowany automatycznie. |
| Protokół | TCP, TCP/UDP lub UDP. |

5.3.3 Host DMZ

Router przekaże pakiety IP z sieci WAN, które nie należą do żadnej z aplikacji skonfigurowanej w tabeli serwerów wirtualnych do komputera hosta DMZ.



Aby aktywować Host DMZ wpisz adres IP hosta i wciśnij **Zastosuj/Zapisz**.

Aby dezaktywować Host DMZ, wyczyść adres IP i wciśnij **Zastosuj/Zapisz**.

5.4 Bezpieczeństwo

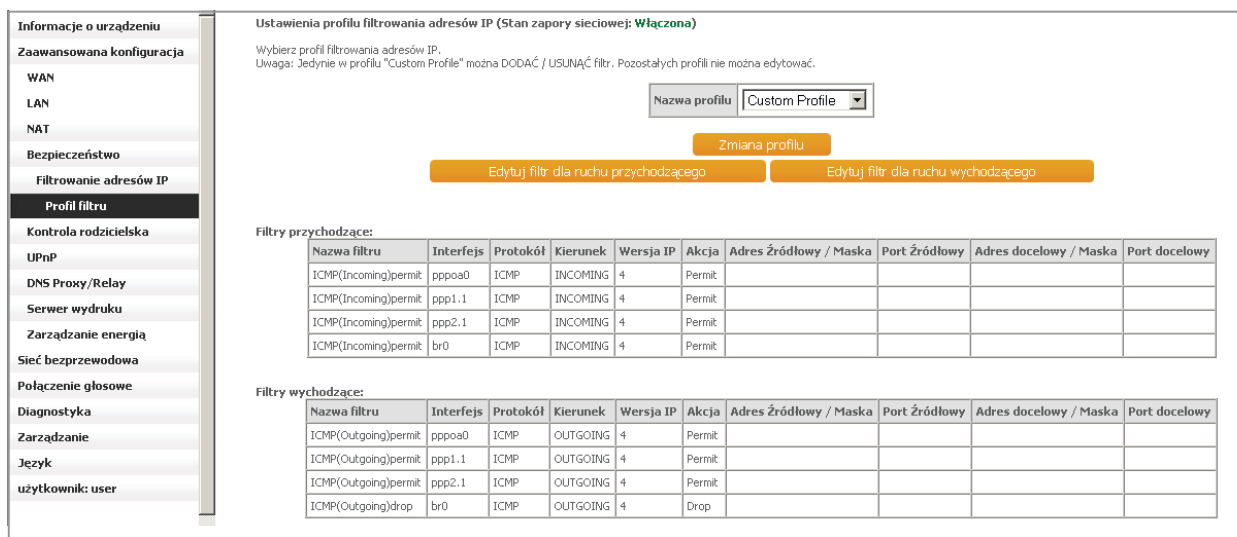
Aby wyświetlić tę funkcję, musisz mieć aktywną zaporę sieciową w menu Zarządzania WAN. Dokładny opis z przykładami znajdziesz w Załącznik A – Zapora sieciowa.

5.4.1 Filtrowanie adresów IP

Ten ekran definiuje reguły, które limitują ruch IP (wychodzący/przychodzący). Może być stworzone wiele reguł, które dotyczą co najmniej jednego warunku. Aby dany pakiet przeszedł filtrowanie, nie może zostać odrzucony przez żaden z filtrów.

Przychodzący i wychodzący filtr IP

Domyślnie, cały ruch IP jest dozwolony, ale może być blokowany filtrami. Kliknij na karcie **Filtrowanie adresów IP**, następnie na **Profil filtru**, aby przywołać następujący ekran.



Wybierz Custom_Profile z menu i kliknij w **Edytuj filtr dla ruchu przychodzącego** lub **Edytuj filtr dla ruchu wychodzącego**.

Ustawienia filtrowania IP dla ruchu przychodzącego

Gdy zaporą sieciową jest włączona na interfejsie WAN lub LAN, wybierz opcję Dodaj lub Usuń aby skonfigurować filtr IP dla ruchu przychodzącego, aby ZEZWALAĆ / BLOKOWAĆ ruch.

Uwaga: Reguła z najniższym priorytetem powinna zostać utworzona jako pierwsza

| Nazwa filtra | Interfejs | Protokół | Wersja IP | Akcja | Adres Źródłowy / Maska | Port Źródłowy | Adres docelowy / Maska | Port docelowy | Usuń |
|----------------------|-----------|----------|-----------|--------|------------------------|---------------|------------------------|---------------|------|
| ICMP(Incoming)permit | ppp0a0 | ICMP | 4 | Permit | | | | | |
| ICMP(Incoming)permit | ppp1.1 | ICMP | 4 | Permit | | | | | |
| ICMP(Incoming)permit | ppp2.1 | ICMP | 4 | Permit | | | | | |
| ICMP(Incoming)permit | br0 | ICMP | 4 | Permit | | | | | |

Aby dodać filtr (blokujący część ruchu wychodzącego lub przychodzącego), wciśnij **Dodaj**.

Na następnym ekranie wpisz kryteria filtru i wciśnij **Zastosuj/Zapisz**.

Dodaj filtr IP - Przychodzące

Ekran ten pozwala na utworzenie reguły filtrowania w celu identyfikacji przychodzącego ruchu IP, poprzez określenie nowej nazwy filtra i co najmniej jednego z warunków poniżej. Wszystkie z wymienionych warunków w tej regule filtrowania muszą być spełnione, aby zasada zadziałała. Kliknij "Zastosuj/Zapisz", aby zapisać i uaktywnić filtr.

Uwaga: Przy konfiguracji określonego adresu IP (w dozwolonej podsieci) aby nie omijać zaporę sieciową, proszę wprowadzić podsieć jako pierwszą w regule zezwalającej na przejście zaporę sieciową. Następnie należy skonfigurować blokowany adres IP w celu pomyślnej implementacji w późniejszy czasie. Jeżeli Użytkownik utworzy inną nazwę filtra, a nazwa ta jest taka sama jak istniejąca nazwa reguły o tym samym kierunku i interfejsie, to zmieni nazwę istniejącej reguły.

Nazwa filtra:

Wersja IP:

Protokół:

Strategia:

Źródłowy adres IP [/ długość prefiksu]:

Port źródłowy (port lub port:port):

Docelowy adres IP [/ długość prefiksu]:

Port docelowy (port lub port:port):

Interfejsy WAN (skonfigurowane w trybie routingu i przy włączonej zaporze sieciowej) i interfejsy LAN
Wybierz jeden lub więcej interfejsów WAN / LAN wyświetlonych poniżej aby zastosować tę zasadę.

- Zastosuj regułę do wszystkich interfejsów
- pppoa_0_0_35/ppp0a0
- pppoe_0_0_1_35/ppp1.1
- pppoe_eth0.35/ppp2.1
- br0/br0
- br0:0/br0:0

W tabeli poniżej znajdziesz opisy poszczególnych pól.

| Nagłówek | Opis |
|------------------------------------|---|
| Nazwa filtra | Wpisz nazwę filtra. |
| Wersja IP | IPv4 wybrane domyślnie. |
| Protokół | TCP, TCP/UDP, UDP lub ICMP. |
| Strategia | Wybierz Allow lub Deny z listy. |
| Źródłowy adres IP | Wpisz źródłowy adres IP |
| Port źródłowy (port lub port:port) | Wpisz port lub zakres portów źródłowych |
| Docelowy adres IP | Wpisz docelowy adres IP |
| Port docelowy (port lub port:port) | Wpisz port lub zakres portów docelowych |

5.5 Kontrola rodzicielska

Ten rozdział opisuje zasady dostępu do Internetu.

5.5.1 Ograniczenia czasu dostępu

Ta opcja blokuje dostęp do sieci zewnętrznej, dla urządzenia sieci lokalnej, przez wybrane dni i czas.



Wybierz **Dodaj** aby przywołać następujący ekran.



Sprawdź opisy pól, kliknij **Zastosuj/Zapisz**, aby kontynuować.

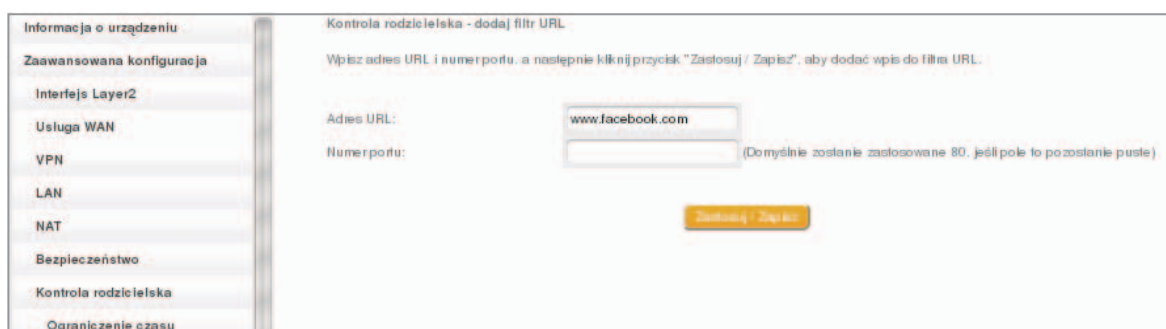
| Nagłówek | Opis |
|------------------------|---------------------------------------|
| Nazwa użytkownika | Twoja nazwa dla tej reguły. |
| Adres MAC przeglądarki | Adres MAC komputera. |
| Inny adres MAC | Adres MAC innego urządzenia |
| Dni tygodnia | Dni działania blokady. |
| Początek blokowania | Czas o którym zaczyna działać blokada |
| Koniec blokowania | Czas końca blokowania |

5.5.2 Filtr URL

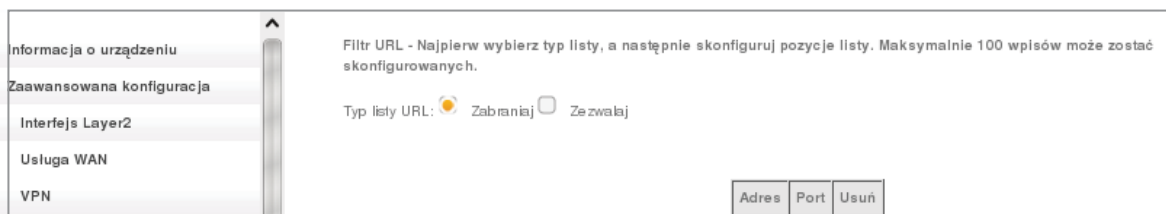
Ten ekran pozwala stworzyć regułę dostępu do stron na podstawie ich adresu URL i numeru portu.



W pierwszej kolejności wybierz rodzaj listy Zabraniaj lub Zezwala, potem kliknij **Dodaj** aby wyświetlić ten ekran.



Wpisz adres URL i numer portu, oraz wciśnij **Zastosuj/Zapisz**. Adresy zaczynają się od WWW, tak jak na przykładzie.



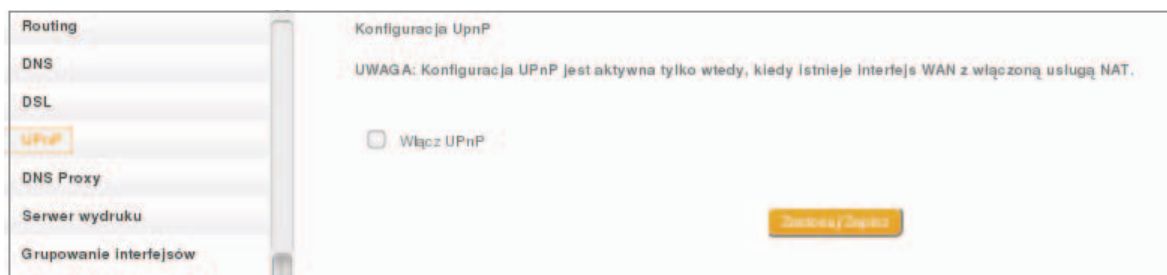
Może być dodane maksymalnie 100 pozycji.

Wybierz przycisk **Zabraniaj**, aby zablokować dostęp do stron poniżej.

Wybierz **Zezwalaj**, aby przyznać dostęp do stron poniżej.

5.6 UPnP

Zaznacz pole i kliknij w **Zastosuj/Zapisz**, aby aktywować protokół UPnP.

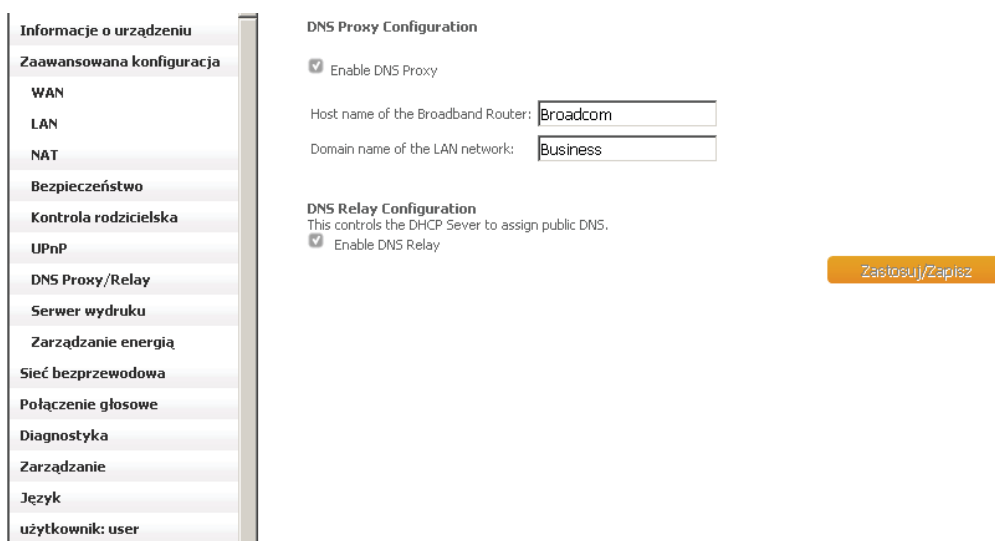


5.7 DNS Proxy/Relay

Strona wyświetla informacje na temat konfiguracji DNS Proxy i DNS Relay.

DNS proxy odbiera zapytania DNS i przekazuje je do Internetu. Po odebraniu odpowiedzi z serwera internetowego, przekazuje odpowiedzi klientom sieci lokalnej. Po skonfigurowaniu Proxy DNS z ustawieniami domyślnymi, komputer w sieci lokalnej otrzyma od serwera DHCP nazwę domeny „Business”, będzie ona dodana do sufiksu wyszukiwania DNS.

DNS Relay, ustawione domyślnie, powoduje przekazywania publicznego DNS przez serwer DHCP



5.8 Serwer wydruku

Router wspiera drukarki podłączone do portu USB2.0. Jeśli twoje urządzenie posiada taki port, sprawdź dokładne instrukcje instalacji w Załącznik B - Specyfikacje.

5.9 Zarządzanie energią

Zarządzanie energią to ważna funkcjonalność, ze względu na:

- Zmniejszenie zużycia energii
- Przedłużenie życia baterii, w przenośnych i wbudowanych urządzeniach
- Zmniejszenie wymagań na chłodzenie
- Zmniejszenie hałasu
- Zmniejszenie kosztów energii i chłodzenia

Mniejsze zużycie energii znaczy mniej wydzielonego ciepła, co zwiększa stabilność systemu i koszty utrzymania. Oszczędza pieniądze i wpływ na środowisko naturalne.

The screenshot shows a web interface for configuring energy management. On the left is a sidebar menu with the following items: 'Informacje o urządzeniu', 'Zaawansowana konfiguracja', 'WAN', 'LAN', 'NAT', 'Bezpieczeństwo', 'Kontrola rodzicielska', 'UPnP', 'DNS Proxy', 'Serwer wydruku', 'Zarządzanie energią' (highlighted), 'Sieć bezprzewodowa', 'Połączenie głosowe', 'Diagnostyka', 'Zarządzanie', 'Język', and 'użytkownik: user'. The main content area is titled 'Zarządzanie energią' and contains the following text: 'Strona ta pozwala na kontrolowanie przez moduły sprzętowe oceny zużycia energii. Użyj przycisków kontrolnych, aby wybrać żadaną opcję, kliknij przycisk Zastosuj i zaznacz odpowiedni status.' Below this is a section 'Instrukcja WAIT w przypadku bezczynności:' with a radio button for 'Włącz' and a status indicator 'Status: Włączona'. Another section 'Wyłącz automatycznie ethernet' has a radio button for 'Włącz' and a status indicator 'Status: Włączona'. To the right of this section, it says 'Liczba interfejsów ethernetowych w: pełnym trybie zasilania: 0 trybie niskiego poboru energii: 5'. At the bottom right of the main area are two buttons: 'Zastosuj' and 'Odśwież'.

Aby aktywować zaznacz odpowiednie pole i wciśnij **Zastosuj**, aby zapisać ustawienia.

Rozdział 6. Sieć bezprzewodowa

Ten rozdział opisuje jak skonfigurować i diagnozować sieci bezprzewodowe.

6.1 Podstawowa konfiguracja

Zakładka **Podstawowa konfiguracja** pozwala na konfigurację podstawowych funkcji bezprzewodowej sieci LAN. Możesz między innymi aktywować lub dezaktywować interfejs bezprzewodowy, ukryć sieć, określić nazwę sieci (SSID) i określić zbiór kanałów, w zależności od twojego kraju.

Sieć bezprzewodowa - ustawienia podstawowe

Ta strona pozwala skonfigurować podstawowe funkcje bezprzewodowego interfejsu LAN. Można włączyć lub wyłączyć interfejs bezprzewodowy LAN, ukryć sieć bezprzewodową przed skanowaniem, ustawić jej nazwę (SSID) oraz ograniczyć zestaw kanałów zgodnie z wymaganiami krajowymi. Kliknij przycisk "Zastosuj / Zapisz", aby zastosować zmiany.

Włącz sieć bezprzewodową
 Ukryj punkt dostępu
 Izolacja klientów
 Wyłącz rozgłaszanie WMM
 Włącz Wireless Multicast Forwarding (WMF)

SSID:

BSSID:

Kraj:

Maksymalna liczba klientów:

Sieć bezprzewodowa - Wirtualne punkty dostępowe:

| Włączona | SSID | Ukryta | Izoluj klientów | Wyłącz rozgłaszanie WMM | Włącz WMF | Maksymalna liczba klientów | BSSID |
|--------------------------|---|--------------------------|--------------------------|--------------------------|--------------------------|---------------------------------|-------|
| <input type="checkbox"/> | <input type="text" value="wl0_Guest1"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="16"/> | N/A |
| <input type="checkbox"/> | <input type="text" value="wl0_Guest2"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="16"/> | N/A |
| <input type="checkbox"/> | <input type="text" value="wl0_Guest3"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="16"/> | N/A |

Wybierz **Zastosuj/Zapisz**, aby zapisać zaznaczone opcje sieci bezprzewodowej.

W tabeli poniżej znajdziesz opisy tych opcji.

| Nagłówek | Opis |
|---|--|
| Włącz sieć bezprzewodową | Pole <input checked="" type="checkbox"/> aktywuje lub dezaktywuje interfejs bezprzewodowej sieci LAN. Po zaznaczeniu, podstawowe opcje pokażą się na ekranie. |
| Ukryj punkt dostępu | Wybierz Ukryj punkt dostępu, aby ukryć nazwę sieci na listach sieci wifi. Aby sprawdzić stan otwórz w Windows XP Połączenia sieciowe , z menu Start , następnie wybierz pokaż dostępne połączenia sieciowe . Jeśli twoja sieć jest ukryta, nie będzie tu widoczna. Aby móc podłączyć do niej swoje urządzenie PC należy skonfigurować ją ręcznie. |
| Izolacja klientów | Aktywowana blokuje dostęp między sobą komputerów będących w sieci lokalnej, w Otoczeniu sieciowym lub Moich Miejscach Sieciowych. Blokuje także inne sposoby komunikacji bezpośredniej. |
| Wyłącz rozgłaszanie WMM | Wyłącza funkcję rozgłaszanie funkcji multimedialnych przez router, ta funkcja pozwala na podstawowe QoS dla aplikacji typu VoIP lub Video. |
| Włącz Wireless Multicast Forwarding (WMF) | Zaznacz pole <input checked="" type="checkbox"/> aby aktywować tą funkcję. |
| SSID | Czas końca blokowania |
| [1-32 znaków] | Ustawia nazwę sieci bezprzewodowej. SSID (ang. Service Set Identifier – Znacznik Zbioru Usług). Wszystkie urządzenia muszą mieć skonfigurowany prawidłowy SSID, aby uzyskać dostęp do sieci. Jeśli nazwa SSID się nie zgadza, użytkownik nie zostanie połączony. |

| | |
|---|--|
| BSSID | BSSID to 48-bitowe słowo, używane do identyfikacji konkretnego BSS (Basic Service Set) w okolicy. W infrastrukturze sieci BSS, jest to adres MAC punktu dostępowego (AP – Access Point). W sieciach niezależnych lub Ad-hoc, jest ono generowane losowo. |
| Kraj | Menu, które udostępnia międzynarodowe i specyficzne lokalne ustawienia. Lokalne regulacje limitują zakresy kanałów: US= wszystkie, Japonia=1-14, Jordan= 10-13, Izrael= 1-13 |
| Maksymalna ilość klientów | Maksymalna liczba klientów, którzy mogą uzyskać dostęp do routera. |
| Sieć bezprzewodowa - Wirtualne punkty dostępowe | Ten router wspiera wiele SSID, zwanych Gościnnymi SSID lub Wirtualnymi punktami dostępowymi. Aby aktywować jeden lub więcej punktów, zaznacz pole <input type="checkbox"/> w kolumnie Włączona . Aby ukryć sieć, zaznacz pole <input type="checkbox"/> w kolumnie Ukryta . Postępuj analogicznie dla ustawień Izolacji klientów , oraz reklamy WMM . Aby uzyskać informację o tych dwóch funkcjach, powróć do poprzedniego punktu. Podobnie, sprawdź informacje o Włącz WMMF , Maksymalna ilość klientów , BSSID w tej tabeli UWAGA: Zdalne urządzenia bezprzewodowe nie mogą skanować Gościnnych SSID. |

6.2 Bezpieczeństwo

Następujący ekran pokazuje się w momencie wybrania zakładki Bezpieczeństwo. Opcje opisane poniżej pozwalają na konfigurację ustawień bezpieczeństwa interfejsu bezprzewodowego sieci lokalnej.

Informacje o urządzeniu

Zaawansowana konfiguracja

Sieć bezprzewodowa

Podstawowa konfiguracja

Bezpieczeństwo

Filtrowanie MAC

Zaawansowana konfiguracja

Informacja o urządzeniach

Połączenie głosowe

Diagnostyka

Zarządzanie

Język

użytkownik: user

Sieć bezprzewodowa - bezpieczeństwo

Ta strona umożliwia skonfigurowanie zabezpieczeń bezprzewodowej sieci LAN. Można ustawić konfigurację ręcznie LUB poprzez WiFi Protected Setup (WPS)

Konfiguracja WPS

Włącz WPS

Ręczna konfiguracja AP

Ustaw metodę uwierzytelnienia, wybierając sposób szyfrowania danych, określając czy klucz szyfrujący jest potrzebny do uwierzytelnienia w tej sieci bezprzewodowej, oraz określając siłę szyfrowania. Kliknij przycisk "Zastosuj / Zapisz", aby zachować zmiany.

Wybierz SSID:

Uwierzytelnianie sieci:

Hasło WPA / WAPI: [Kliknij tutaj, aby wyświetlić](#)

Okres odnawiania klucza grupowego WPA:

Szyfrowanie WPA / WAPI:

Szyfrowanie WEP:

Wybierz **Zastosuj/Zapisz**, aby zapisać nowe ustawienia.

Konfiguracja zabezpieczeń sieci bezprzewodowej

Ustawienia bezpieczeństwa sieci bezprzewodowej mogą być skonfigurowane zgodnie ze standardem WPS (Wi-Fi protected setup) lub ręcznie. Metoda WPS pozwala skonfigurować ustawienia bezprzewodowe automatycznie (sprawdź rozdział 6.2.1 WPS), podczas gdy metoda ręczna wymaga ustawienia wszystkich opcji z użyciem interfejsu WWW (informacje w tabeli poniżej).

Wybierz SSID

Wybierz nazwę sieci z listy. SSID to Identyfikator sieci. Wszystkie urządzenia muszą mieć skonfigurowany prawidłowy SSID, aby uzyskać dostęp do sieci. Jeśli nazwa SSID się nie zgadza, użytkownik nie zostanie połączony.

Uwierzytelnianie sieci

Ta opcja definiuje, czy klucz sieciowy jest używany do uwierzytelniania do sieci bezprzewodowej. Jeśli uwierzytelnianie jest ustawione na Open, nie używa się klucza. Pomimo tego identyfikacja klienta jest wciąż sprawdzana.

Każdy typ uwierzytelniania ma swoje ustawienia. Na przykład wybranie uwierzytelniania 802.1X wyświetli ustawienia adresu IP, portu i klucza serwera RADIUS. Szyfrowanie WEP będzie również aktywowane, jak pokazano poniżej.

| | |
|--------------------------|---------------|
| Uwierzytelnianie sieci: | 802.1X |
| Adres IP serwera RADIUS: | 0.0.0.0 |
| Port RADIUS: | 1812 |
| Klucz RADIUS: | |
| Szyfrowanie WEP: | Enabled |
| Siła szyfrowania: | 128-bit |
| Bieżący klucz sieciowy: | 2 |
| Klucz sieciowy 1: | 1234567890123 |
| Klucz sieciowy 2: | 1234567890123 |
| Klucz sieciowy 3: | 1234567890123 |
| Klucz sieciowy 4: | 1234567890123 |

Wprowadź 13 znaków ASCII lub 26 cyfr szesnastkowych dla 128-bitowych kluczy szyfrowania
Wprowadź 5 znaków ASCII lub 10 cyfr szesnastkowych dla 64-bitowych kluczy szyfrowania

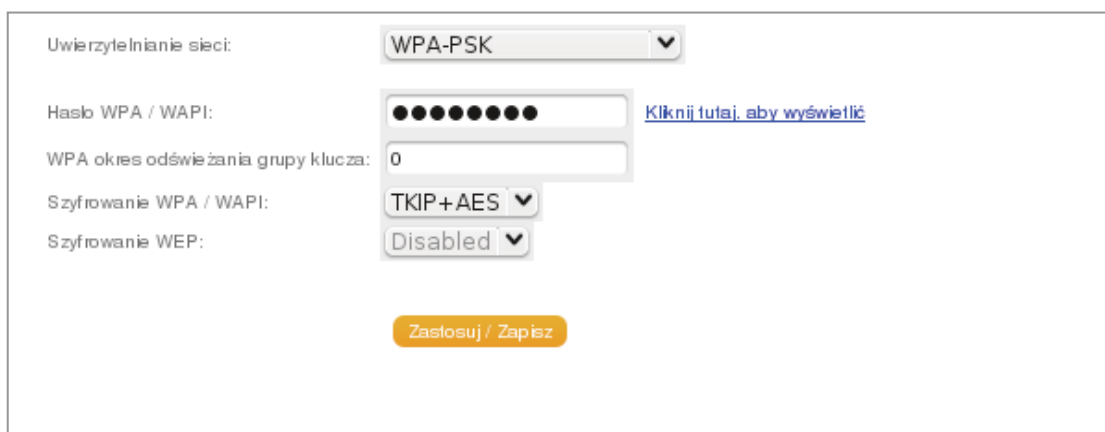
Zastosuj / Zapisz

Ustawienia dla WPA są pokazane na następnym ekranie.

| | |
|-------------------------------------|----------|
| Uwierzytelnianie sieci: | WPA |
| WPA okres odświeżania grupy klucza: | 0 |
| Adres IP serwera RADIUS: | 0.0.0.0 |
| Port RADIUS: | 1812 |
| Klucz RADIUS: | |
| Szyfrowanie WPA / WAPI: | TKIP+AES |
| Szyfrowanie WEP: | Disabled |

Zastosuj / Zapisz

Następnie, ustawienia WPA-PSK



The screenshot shows a configuration interface for WPA-PSK. It includes the following fields and controls:

- Uwierzytelnianie sieci:** A dropdown menu set to "WPA-PSK".
- Hasło WPA / WAPI:** A text input field with 10 black dots representing a password. To its right is a blue link: [Kliknij tutaj, aby wyświetlić](#).
- WPA okres odświeżania grupy klucza:** A text input field containing the value "0".
- Szyfrowanie WPA / WAPI:** A dropdown menu set to "TKIP+AES".
- Szyfrowanie WEP:** A dropdown menu set to "Disabled".
- Zastosuj / Zapisz:** An orange button at the bottom center.

Hasło WPA/WAPI

Sekwencja słów lub innego tekstu, pozwala uzyskać bezpieczny dostęp.

Okres odświeżania grupy klucza

Domyślne to "0"

Szyfrowanie WPA/WAPI

AES lub TKIP+AES, domyślny to AES

Szyfrowanie WEP

Ta opcja ustala czy dane są przesyłane po sieci w postaci zaszyfrowanej. Ten sam klucz jest używany do uwierzytelniania i szyfrowania. Cztery klucze mogą być zdefiniowane, ale tylko jeden może być używany jednocześnie. Użyj listy Obecny Klucz sieciowy, aby wybrać odpowiedni klucz.

Opcje bezpieczeństwa to między innymi usługi uwierzytelniania i szyfrowania oparte na algorytmie WEP. WEP to zbiór usług bezpieczeństwa używanych do zabezpieczania sieci 802.11 przed nieautoryzowanym dostępem, podsłuchiwaniami.

W tym przypadku dokładnie chodzi o przechwytywanie ruchu sieciowego. Podczas gdy aktywowane jest szyfrowanie danych, tajne klucze szyfrowania są tworzone i używane przez stacje źródłowe i docelowe do ukrywania ramek bitowych, czyli ukrywania danych przed podsłuchującymi.

W trybie współdzielonego klucza, każde urządzenie musi otrzymać tajny współdzielony klucz bezpiecznym kanałem, czyli na przykład innym niż kanał komunikacyjny sieci 802.11.

Siła szyfrowania

Ta lista wyświetli się, gdy szyfrowanie WEP jest aktywowane. Siła klucza jest proporcjonalna do liczby bitów z których składa. To znaczy, że dłuższe klucze odznaczają się większym poziomem bezpieczeństwa i są znacznie trudniejsze do złamania. Siła szyfrowania może być ustawiona na 64 lub 128 bitów. Klucz 5-bitowy to 5 znaków ASCII lub 10 liczb szesnastkowych. Klucz 128 bitowy, składa się z 13 znaków ASCII lub 26 liczb szesnastkowych. Każdy klucz zawiera 24-bitowy nagłówek (tak zwany wektor inicjujący) który pozwala na równoległe dekodowanie wielu strumieni zaszyfrowanych danych.

6.2.1 WPS

Wi-Fi Protected Setup (WPS), czyli Bezpieczna konfiguracja Wi-Fi, to standard który ułatwia konfigurację ustawień bezpieczeństwa wspierającym go urządzeniom sieciowym. Każde certyfikowane urządzenie WPS posiada numer PIN i przycisk zlokalizowany na urządzeniu lub dostępny przez oprogramowanie. Router posiada przycisk na obudowie i wirtualny przycisk osiągalny przez interfejs WWW.

Urządzenia z logo WPS (po prawej) wspierają WPS. Jeśli logo nie jest obecne na urządzeniu, może mimo wszystko wspierać WPS, w takim przypadku sprawdź dokumentację pod kątem hasła „Wi-Fi protected Setup”



UWAGA: WPS jest dostępny jedynie w trybie Open, WPA-PSK, WPA2-PSK oraz mieszanym WPA2/WPA-PSK. Inne tryby uwierzytelniania nie używają WPS, czyli muszą być konfigurowane ręcznie.

Aby skonfigurować ustawienia z użyciem WPS, postępuj według procedury poniżej. **Musisz wybrać metodę wciśnięcia przycisku lub konfigurację kodem PIN dla kroków 6 i 7.**

I. Konfiguracja

KROK 1: Aktywuj WPS, przez wybranie Enabled z listy Włącz WPS.

The screenshot shows the 'Konfiguracja WPS' (WPS Configuration) page. At the top, 'Włącz WPS' (Enable WPS) is set to 'Enabled'. Below this, there is a section for adding a client, with three radio button options: 'Przycisk' (Push button), 'Wprowadź PIN STA' (Enter PIN STA), and 'Użyj PIN AP' (Use PIN AP). A 'Dodaj Enrollee' button is present. The 'Ustaw tryb WPS AP' (Set WPS AP mode) dropdown is set to 'Configured'. Below that, there is a 'Konfiguruj AP' (Configure AP) section with a note: '(skonfiguruj wszystkie ustawienia zabezpieczeń z zewnętrznym rejestrzem)'. The 'PIN urządzenia' (Device PIN) field contains '10864111' and has a 'Help' link. A 'Konfiguracja AP' button is at the bottom.

KROK 2: Ustaw tryb WPS AP. Configured jest używany, gdy router przyzna ustawienia bezpieczeństwa klientom. Unconfigured odpowiada sytuacji odwrotnej, gdy klient zewnętrzny przydziela ustawienia routerowi.

UWAGA: Twój klient niekoniecznie musi mieć możliwość przydzielenia ustawień bezpieczeństwa routerowi. Jeśli nie posiada takiej funkcjonalności, musisz ustawić tryb WPS AP w Configured. Sprawdź dokumentację urządzenia aby sprawdzić jego możliwości.

Dodatkowo, używając Windows Vista, możesz dodać zewnętrzny rejestrator używając przycisku StartAddER (Załącznik C – Zewnętrzny Rejestrator WPS).

II. Uwierzytelnianie sieciowe

KROK 3: Wybierz Open, WPA-PSK, WPA2-PSK lub mieszany WPA2/WPA-PSK z listy trybów uwierzytelniania sekcji ręcznej konfiguracji AP, ekranu bezpieczeństwa bezprzewodowego. Przykład poniżej pokazuje przypadek WPA2-PSK.

Ręczna konfiguracja AP

Można ustawić metodę uwierzytelniania sieci, wybierając szyfrowanie danych.
Określ, czy klucz sieciowy jest wymagany do uwierzytelniania w sieci bezprzewodowej i określ sposób szyfrowania.
Kliknij przycisk "Zastosuj / Zapisz" po zakończeniu.

Wybierz SSID:

Uwierzytelnianie sieci:

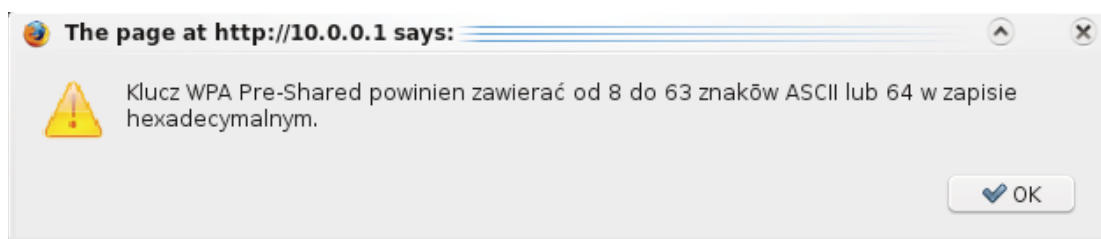
Hasło WPA / WAPI: [Kliknij tutaj, aby wyświetlić](#)

WPA okres odświeżania grupy klucza:

Szyfrowanie WPA / WAPI:

Szyfrowanie WEP:

KROK 4: Dla trybu PSK (klucz współdzielony) wpisz klucz WPA. Zobaczysz następujące okno dialogowe, jeśli klucz jest zbyt krótki lub zbyt długi.



KROK 5: Kliknij Zastosuj/Zapisz na dole ekranu.

IIIa. Konfiguracja z użyciem przycisku

Przycisk WPS, pozwala na półautomatyczną konfigurację. Przycisk z tyłu urządzenia lub konfiguracja za pomocą strony WWW mogą być używane zamiennie.

Procedura konfiguracji przycisku WPS jest opisana poniżej. Zostało przyjęte założenie, że funkcja sieci bezprzewodowej jest aktywowana, oraz że router jest skonfigurowany jako AP (Access Point) sieci WLAN. Dodatkowo, klient musi być również skonfigurowany poprawnie i mieć aktywowaną funkcję WPS.

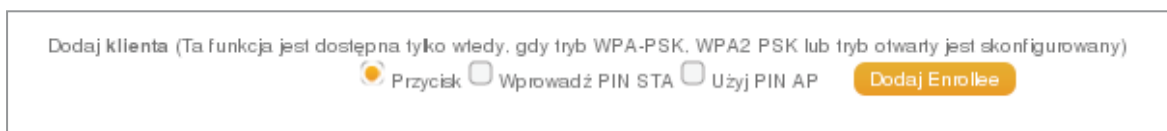
UWAGA: Router wyszukuje klientów przez 2 minuty, jeśli router zaprzestanie poszukiwań zanim ukończysz krok 7, powróć do kroku 6.

KROK 6: Pierwsza metoda: przycisk WPS

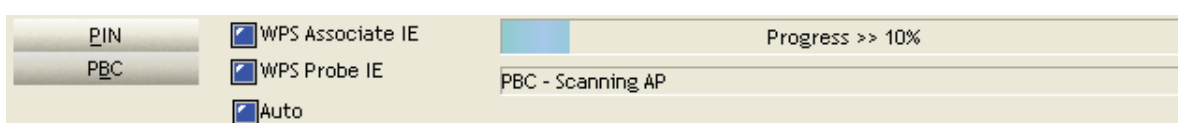
Wciśnij przycisk WPS na tylnej części obudowy. Lampka LED WPS zacznie migać, sygnalizując, że router rozpoczął poszukiwanie klientów.

Druga metoda: wirtualny przycisk interfejsu WWW

Zaznacz **Przycisk** w sekcji WSC ekranu bezpieczeństwa bezprzewodowego i kliknij **Dodaj Enrollee**.



KROK 7: W twoim kliencie WPS aktywuj funkcję przycisku. Standardowy, przykładowy klient WPS jest pokazany poniżej.



Teraz udaj się do kroku 8 (część IV sprawdź konfigurację), aby sprawdzić połączenie WPS.

IIIb. WPS – Ustawienia PIN

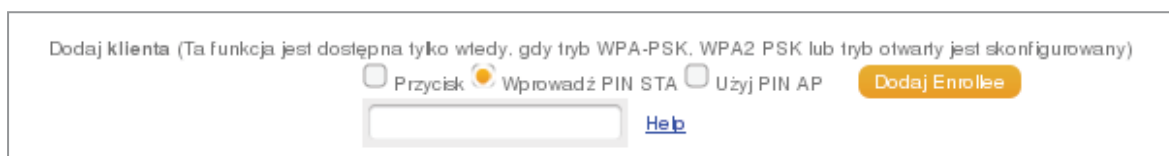
Używając tej metody, ustawienia bezpieczeństwa są konfigurowane z użyciem osobistego numeru PIN. Ten numer może być umieszczony na urządzeniu lub w oprogramowaniu. W drugim przypadku może on być wygenerowany losowo. Aby uzyskać numer PIN twojego klienta, sprawdź dokumentację urządzenia.

Konfiguracja kodu PIN dla WPS jest opisana poniżej. Zostało przyjęte założenie, że funkcja sieci bezprzewodowej jest aktywowana, oraz że router jest skonfigurowany jako AP (Access Point) sieci WLAN. Dodatkowo, klient musi być również skonfigurowany poprawnie i włączony z aktywowaną funkcją WPS.

UWAGA: W przeciwieństwie do metody przycisku WPS, metoda PIN nie ma ustanowionego limitu czasowego. Znaczy to tyle, że router będzie poszukiwał klienta do skutku.

KROK 6: Wybierz Wprowadź **PIN STA** w sekcji ustawień WSC ekranu bezpieczeństwa bezprzewodowego, jak w opcji **A** lub **B** poniżej, następnie kliknij odpowiedni przycisk, wybrany w kroku 2.

A – W trybie **Configured** wybierz Wprowadź PIN STA i wpisz kod PIN dla klienta (czyli urządzenia które podłączy się do sieci). Następnie wciśnij przycisk **Dodaj Enrollee**.



B – w trybie Unconfigured, po wybraniu trybu z listy wybierz Zastosuj/Zapisz. Skopiuj kod PIN urządzenia i wklej je do aplikacji klienta. Klient musi być skonfigurowany jako Zewnętrzny Rejestrator WPS. Kliknij przycisk Konfiguracja AP.



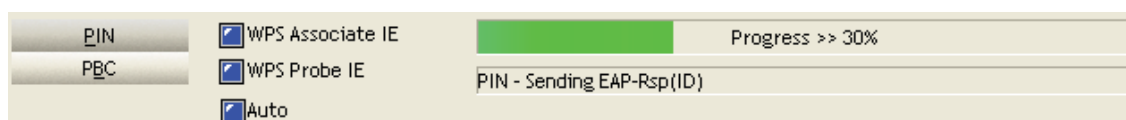
The screenshot shows a configuration window with a label 'PIN urządzenia' on the left. To its right is a text input field containing the number '10864111'. Further right is a blue 'Help' link. Below these elements is a yellow button with the text 'Konfiguracja AP'.

UWAGA: Aktywowanie kodu PIN na kliencie bezprzewodowym.

W trybie Configured, klient musi być skonfigurowany jako Enrollee.

W trybie Unconfigured, klient musi być skonfigurowany jako Zewnętrzny Rejestrator WPS. Jest to inna funkcja niż funkcjonalność External Registrar w Windows Vista.

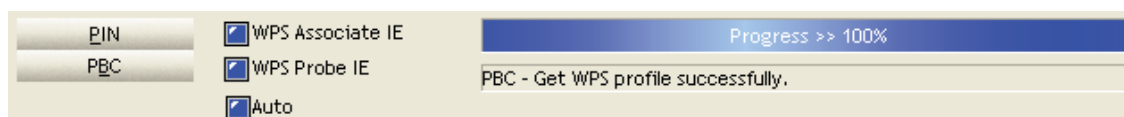
Ekran poniżej przedstawia przykładowego klienta WPS w trakcie trwania funkcji PIN WPS.



Następnie przejdź do kroku 8 (część IV. Sprawdź połączenie) aby sprawdzić połączenie WPS.

IV. Sprawdź połączenie

KROK 8: Jeśli metoda konfiguracji WPS zakończyła się sukcesem, będziesz w stanie uzyskać dostęp do sieci bezprzewodowej. Aplikacja klienta zakomunikuje ten stan. Przykład poniżej pokazuje ekran klienta WPS po zakończeniu ustanawiania połączenia.



Możesz również kliknąć dwukrotnie ikonę Połączenia Bezprzewodowego w oknie Połączeń Sieciowych (lub zasobniku systemowym) aby sprawdzić stan nowego połączenia.

6.3 Filtrowanie MAC

Opcja ta pozwala zastrzec dostęp do routera na podstawie adresów MAC urządzeń bezprzewodowych. Aby dodać filtr MAC adresu, kliknij przycisk Dodaj, pokazany na poniższym ekranie. Aby usunąć filtr MAC adresu, wybierz go z tabeli filtrów MAC adresów i kliknij przycisk usuń pokazany na poniższym ekranie.

Informacje o urządzeniu
Zaawansowana konfiguracja
Sieć bezprzewodowa
Podstawowa konfiguracja
Bezpieczeństwo
Filtrowanie MAC
Zaawansowana konfiguracja
Informacja o urządzeniach
Połączenie głosowe
Diagnostyka
Zarządzanie
Język
użytkownik: user

Sieć bezprzewodowa - filtrowanie MAC

Wybierz SSID:

Filtrowanie MAC: Wyłączone Zezwalaj Blokuj

| Adres MAC | usuń |
|-----------|------|
|-----------|------|

| Opcja | Opis |
|-----------------|--|
| Wybierz SSID | Wybierz nazwę sieci bezprzewodowej z rozwijanej listy. SSID (Service Set Identifier) jest nazwą współdzieloną przez wszystkie urządzenia w sieci bezprzewodowej. Wszystkie urządzenia w Twojej sieci bezprzewodowej muszą mieć ustawione odpowiednie SSID. Jeśli nazwy SSID nie będą takie same, urządzenie nie uzyska dostępu do sieci WLAN. |
| Filtrowanie MAC | Wyłączony: Filtrowanie adresów MAC jest wyłączone. Zezwalaj: Zezwalaj na dostęp urządzeniom o wybranych adresach MAC. Odmawiaj: Odmawiaj dostępu urządzeniom o wybranych adresach MAC. |
| Adres MAC | Lista adresów MAC w zależności od wybranej opcji. Można dodać maksymalnie 60 adresów MAC. Każde urządzenie sieciowe ma unikalny 48-bitowy adres MAC. Wyświetla się go jako xx.xx.xx.xx.xx.xx, gdzie xx są liczbami zapisanymi w kodzie szesnastkowym. |

Po kliknięciu na przycisk **Dodaj** pojawi się ekran, jak poniżej.

Informacje o urządzeniu
Zaawansowana konfiguracja
Sieć bezprzewodowa
Podstawowa konfiguracja
Bezpieczeństwo
Filtrowanie MAC
Zaawansowana konfiguracja
Informacja o urządzeniach
Połączenie głosowe
Diagnostyka
Zarządzanie
Język
użytkownik: user

Sieć bezprzewodowa - filtrowanie MAC

Wpisz adres MAC i kliknij przycisk "Zastosuj / Zapisz", aby dodać ten adres do listy filtrowanych adresów MAC sieci bezprzewodowej.

Adres MAC:

Wprowadź adres MAC w odpowiednie pole i kliknij przycisk **Zastosuj/Zapisz**.

6.4 Zaawansowana konfiguracja

Zakładka ta umożliwia sprawdzenie konfiguracji zaawansowanych funkcji interfejsu sieci bezprzewodowej.

| | |
|----------------------------------|--|
| Informacje o urządzeniu | Wireless -- Advanced (For User Level) This page let you to Know advanced features of the wireless LAN interface. If You want to modify Configutre, you need login with "Root" Account. |
| Zaawansowana konfiguracja | |
| Sieć bezprzewodowa | |
| Podstawowa konfiguracja | |
| Bezpieczeństwo | |
| Filtrowanie MAC | |
| Zaawansowana konfiguracja | |
| Informacja o urządzeniach | |
| Połączenie głosowe | |
| Diagnostyka | |
| Zarządzanie | |
| Język | |
| użytkownik: user | |
| | |

| Pole | Opis |
|------------------------------------|---|
| Pasmo | Ustawiono na 2.4 GHz aby zachować kompatybilność ze standardami IEEE 802.11x. Nowy standard IEEE 802.11n pozwala również na pracę z mniejszymi przepływnościami, tak by starsze urządzenia zgodne ze standardem IEEE 802.11b lub g mogły współistnieć w tej samej sieci. Standard IEEE 802.11a ma pewne różnice w porównaniu do standardu IEEE 802.11b lub g, np. oferując więcej kanałów. Nie jest on jednak stosowany w Europie |
| Kanał | Rozwijane menu pozwala wybrać konkretny kanał. |
| Automatyczny timer kanałów (min) | Automatyczny timer kanałów w minutach (0 oznacza wyłączony) |
| 802.11n/EWC | Standard współdzielenia sieci oparty na IEEE 802.11n Draft 2.0 oraz Enhanced Wireless Consortium (EWC) |
| Przepustowość | Pasmo 20GHz lub 40GHz. Pasmo 40GHz wykorzystuje dwa sąsiednie pasma 20GHz dla zwiększonej przepustowości. |
| Kontrola wstęgi | W przypadku wyboru pasma 40 GHz wybierz wstęgę Górną lub Dolną. |
| Wskaźnik 802.11n | Wybierz physical transmission rate (PHY). |
| Zabezpieczenie 802.11n | Wyłącz dla maksymalnej przepustowości. Włącz dla lepszego bezpieczeństwa. |
| Wsparcie 802.11n tylko dla klienta | Wyłącz aby urządzenia standardu 802.11b/g miały dostęp do routera. Włącza aby uniemożliwić urządzeniom standardu 802.11b/g dostęp do routera. |
| Reklama RIFS | Reduced Interframe Space (RIFS) jest techniką tworzenia krótkich opóźnień pomiędzy PDU aby zwiększyć wydajność łączności bezprzewodowej. |
| Koegzystencja OBSS | Koegzystencja pomiędzy 20 MHz i 40 MHz Overlapping Basic Service Set (OBSS) w sieci WLAN. |
| Chain RX Oszczędzanie mocy | Włączenie tej opcji umożliwia oszczędzenie energii poprzez wyłączenie Chain RX (przejdzie z 2x2 na 2x1). |

| | |
|---|--|
| Chain RX Oszczędzanie czasu | Ilość sekund , przez które ruch musi być poniżej wartości PPS aby aktywowała się opcja Chain RX Oszczędzanie mocy . |
| RX Chain PPS Oszczędzanie energii | Maksymalna ilość pakietów na sekundę, które mogą być przetworzone przez interfejs WLAN podczas Oszczędzania czasu (opisanego powyżej) zanim włączy się opcja RX Chain PPS Oszczędzanie energii. |
| Wskaźnik 54g™ | Rozwijane menu zawierające stałe szybkości: Auto: Domyślne. Jeśli możliwe używa przepustowości 11 Mb/s ale w razie potrzeby zmniejsza przepustowość. Stałe szybkości 1 Mb/s, 2 Mb/s, 5.5 Mb/s i 11Mb/s. Odpowiednie ustawienie jest zależne od siły sygnału. |
| Szybkość multimiisji | Ustawienie Szybkość multimiisji pakietów (1-54 Mb/s) |
| Szybkość podstawowa | Ustawienie szybkości podstawowej. |
| Próg fragmentacji | Próg fragmentacji, określony w bajtach, określa, czy pakiety podlegną fragmentacji i rozmiar tych fragmentów. W 802.11 WLAN, pakiety, które przekraczają próg fragmentacji podlegają fragmentacji tzn. podzieleniu na mniejsze fragmenty odpowiednie dla obiegu danych. Pakiety mniejsze od określonego progu fragmentacji nie podlegają fragmentacji. Należy wprowadzić wartość pomiędzy 256 i 2346. Jeśli doświadczysz dużego wskaźnika straty pakietów spróbuj nieznacznie zwiększyć próg fragmentacji. Wartość powinna pozostać na swoim domyślnym poziomie 2346. Ustawienie progu fragmentacji na za niskim poziomie może skutkować niską wydajnością. |
| Próg RTS | Request to Send, gdy ustawiony w bajtach, określa rozmiar pakietu poza którym karta WLAN uruchomi swój mechanizm RTS/CTS. Pakiety, które przekraczają określony próg RTS wyzwalają mechanizm RTS/CTS. NIC przesyła mniejsze pakiety bez użycia mechanizmu RTS/CTS. Domyślna wartość progu RTS 2347 (maksymalna długość pakietu) wyłącza próg RTS. |
| Interwał DTIM | Delivery Traffic Indication Message (DTIM) zwany jest także wskaźnikiem sygnału identyfikacji. Przyjmuje wartości od 1 do 65535. DTIM jest odliczaną w dół zmienną, która informuje klienta o następnym przedziale czasu, w którym należy oczekiwać kolejnych wiadomości nadawanych lub wiadomości multimiisji. Gdy AP zbuforuje te wiadomości dla odpowiednich klientów, wysyła kolejny DTIM z interwałem DTIM. Klienci AP otrzymując ten sygnał przygotowują się do odbioru wiadomości. Domyślna wartość Interwału DTIM wynosi 1. |
| Przedział czasowy pomiędzy transmisjami sygnału identyfikacji | Czas pomiędzy kolejnymi transmisjami sygnału identyfikacji w milisekundach. Domyślna wartość wynosi 100 ms (powinna przyjmować wartości od 1 do 65535). Wysłanie sygnału identyfikacji identyfikuje obecność punktu dostępowego AP. Wszystkie urządzenia sieciowe, domyślnie, skanują wszystkie kanały RF w poszukiwaniu sygnału identyfikacji AP. Zanim stacja przejdzie w tryb oszczędzania energii musi znać wartość przedziału czasowego pomiędzy transmisjami sygnału identyfikacji aby wiedzieć kiedy ponownie wyjść z trybu oszczędzania energii by odebrać kolejny sygnał identyfikacji, oraz dowiedzieć się czy na AP nie oczekują dla niej zbuforowane ramki danych. |
| Maksymalna liczba klientów globalnych | Maksymalna liczba klientów, którzy mogą być podłączeni do rutera. |
| Technologia XPress™ | Technologia Xpress jest zgodna z projektami specyfikacji dwóch nadchodzących standardów bezprzewodowych. |
| Moc nadawania | Ustawia określoną moc nadawania (w procentach). |
| WMM (Wi-Fi Multimedia) | Technologia ta umożliwi usługom audio, video, aplikacjom głosowym i innym usługom multimedialnym uzyskanie wyższego priorytetu w sieci Wi-Fi. |
| Brak potwierdzenia WMM | Odnosi się do polityki potwierdzania wysyłanych i odebranych danych na poziomie MAC. Włączając Brak potwierdzenia WMM może spowodować bardziej wydajną transmisję ale wyższym wskaźnikiem błędów w środowisku od dużym ruchu radiowym. |
| APSD WMM | Opcja automatycznego oszczędzania energii. |

6.5 Informacje o urządzeniach

Ta strona pokazuje uwierzytelnione stacje bezprzewodowe i ich status. Kliknij przycisk Odśwież aby odświeżyć listę stacji w sieci WLAN.

Sieć bezprzewodowa - uwierzytelnione stacje

Ta strona pokazuje uwierzytelnione stacje bezprzewodowe oraz ich status.

| MAC | Połączony | Autoryzowany | SSID | Interfejs |
|-------------------|-----------|--------------|------------------------|-----------|
| 00:12:F0:22:9E:15 | Yes | Yes | COMTREND-VI-3223u-AA29 | wl0 |

Odśwież

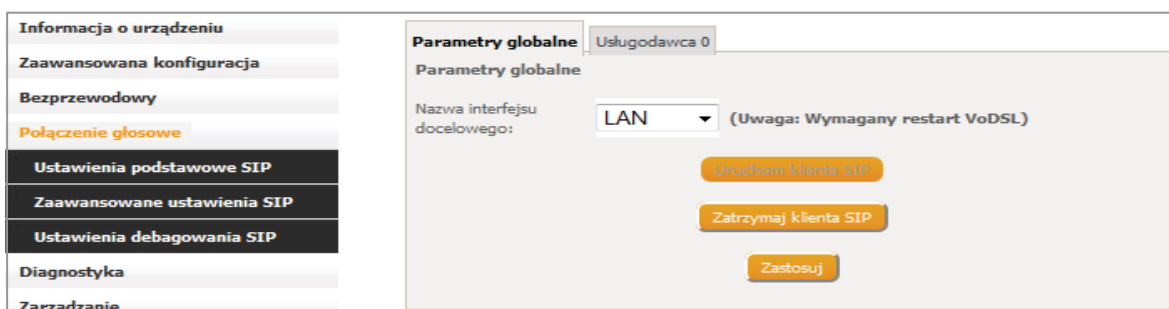
Poniższa tabela zawiera opis każdego nagłówka powyższej tabeli.

| Nagłówek | Opis |
|--------------|---|
| MAC | Adresy MAC wszystkich stacji. |
| Połączony | Wszystkie stacje powiązane z AP oraz ilość czasu, która upłynęła od ostatniej transmisji pakietów od lub do stacji. Jeśli stacja jest nieaktywna przez dłuższy okres czasu, jest usuwana z listy. |
| Autoryzowany | Urządzenia z autoryzowanym dostępem. |
| SSID | SSID modemu, do którego podłączone są stacje. |
| Interfejs | Interfejs modemu, do którego są podłączone stacje. |

Rozdział 7. Połączenia głosowe

Na początku tego rozdziału opisane zostaną różne opcje konfiguracji usług głosowych SIP. Następnie pokazane zostaną szczegółowe instrukcje dotyczące połączeń głosowych wykorzystujących usług VoIP (Voice over IP) oraz PSTN (Public Switched Telephone Network).

Session Initiation Protocol (SIP) jest protokołem peer-to-peer wykorzystywanym w Internecie do konferencji, telefonii, powiadamianiu o zdarzeniach i wiadomościach natychmiastowych. SIP został zaprojektowany do zarządzania funkcjami sygnalizacji i zarządzania sesją w sieci pakietowej. Sygnalizacja pozwala na przeniesienie informacji o połączeniu poza granice sieci. Zarządzanie sesją zapewnia możliwość kontroli właściwości połączeń end-to-end.



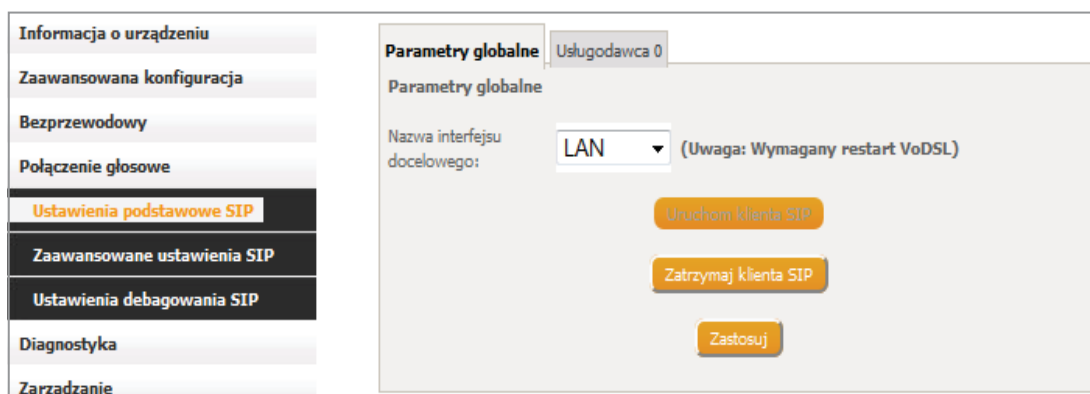
UWAGA: Standard SIP został ustanowiony przez Internet Engineering Task Force (IETF).

Standard SIP definiuje następujących urządzenia agent/serwer:

- User Agents (UA) – Klient telefoniczny SIP (fizyczny lub softwareowy)
- Proxy Server – transmituje dane pomiędzy UA i zewnętrznymi serwerami
- Registrar Server – serwer akceptujący żądania rejestracji od UA
- Redirect Server – zapewnia funkcje wyszukiwania adresów dla UA

Poniżej zostały przedstawione kolejne ekrany konfiguracji SIP (Ustawienia Podstawowe, Zaawansowane i Ustawienia Debugowania). Każdy ekran pokazuje zróżnicowane opcje konfiguracji SIP.

7.1 Ustawienia Podstawowe SIP



7.1.1 Parametry globalne

Ustawienia podstawowych parametrów.

Parametry globalne Usługodawca 0

Parametry globalne

Nazwa interfejsu docelowego: (Uwaga: Wymagany restart VoDSL)

Uruchom klienta SIP

Zatrzymaj klienta SIP

Zastosuj

7.1.2 Usługodawca

Poniższy ekran przedstawia podstawowe ustawienia konfiguracji SIP.

Parametry globalne | **Usługodawca 0**

Połączenie głosowe - konfiguracja SIP

Wprowadź parametry SIP i kliknij przycisk Start / Stop, aby zapisać parametry i uruchomić / zatrzymać aplikację głosową.

Wybór ustawień*: **USA - NORTHAMERICA** ▾ (Uwaga: Wymagany restart VoDSL)

Nazwa domeny SIP*:

Cyfry Max Ustawianie:

Użyj serwera proxy SIP.

Użyj wychodzącego serwera proxy SIP.

| Konto SIP | 0 | 1 |
|------------------------|--|--|
| Konto włączone | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Przedłużenie | <input type="text" value="1001"/> | <input type="text" value="2001"/> |
| Wyświetlana nazwa | <input type="text" value="1001"/> | <input type="text" value="2001"/> |
| Nazwa uwierzytelniania | <input type="text"/> | <input type="text"/> |
| Hasło | <input type="text" value="...."/> | <input type="text" value="...."/> |
| Preferowanyptime | <input type="text" value="20"/> ▾ | <input type="text" value="20"/> ▾ |
| Preferowany kodek 1 | <input type="text" value="G.711ALaw"/> ▾ | <input type="text" value="G.711ALaw"/> ▾ |
| Preferowany kodek 2 | <input type="text" value="G.729a"/> ▾ | <input type="text" value="G.729a"/> ▾ |
| Preferowany kodek 3 | <input type="text" value="G.723.1"/> ▾ | <input type="text" value="G.723.1"/> ▾ |
| Preferowany kodek 4 | <input type="text" value="G.726_24"/> ▾ | <input type="text" value="G.726_24"/> ▾ |
| Preferowany kodek 5 | <input type="text" value="G.726_32"/> ▾ | <input type="text" value="G.726_32"/> ▾ |
| Preferowany kodek 6 | <input type="text" value="AMR_WB_66"/> ▾ | <input type="text" value="AMR_WB_66"/> ▾ |

* Zmiana tego parametru dla jednego usługodawcy wpłynie na ustawienia wszystkich innych dostawców usług.

Po skonfigurowaniu ustawień kliknij przycisk **Zastosuj**, aby rozpocząć korzystać z usługi.

| Pole | Opis |
|---|---|
| Wybór ustawień | Określa ton, rodzaj dzwonka i fizyczne parametry specyficzne dla danego kraju. |
| Nazwa domeny SIP | Dostarczone przez Twojego dostawcę VoIP. |
| Cyfry Max Ustawianie | Określa maksymalną liczbę numerów, które mogą być wykręcone. |
| Użyj serwera proxy SIP | Włącz serwer SIP proxy zaznaczając pole wyboru <input type="checkbox"/> i ustawiając parametry serwera proxy. |
| Serwer proxy SIP | Adres IP albo nazwa domeny serwera proxy SIP, używana przez dostawcę VoIP. |
| Port serwera proxy SIP | Ustalony przez dostawcę VoIP. |
| Użyj wychodzącego serwera proxy SIP | Zaznacz jeśli wymaga tego dostawca VoIP. Włącz opcję wychodzącego serwera proxy SIP zaznaczając pole wyboru i ustawiając parametry wychodzącego serwera proxy SIP. Jeśli nie można skontaktować się bezpośrednio z serwerem proxy SIP, wiadomości są przekazywane dalej przez wychodzący serwer proxy SIP. |
| Wychodzący serwer proxy SIP | Adres IP wychodzącego serwera proxy SIP. |
| Port wychodzącego serwera proxy SIP | Port wychodzącego serwera proxy SIP. |
| <p>UWAGA: Serwer proxy jest programem pośredniczącym, który zachowuje się jednocześnie jak klient i serwer aby wysłać żądania w imieniu innych klientów. Żądania są przetwarzane wewnętrznie albo wysyłane do innych serwerów. Serwer proxy interpretuje i jeśli to konieczne, przepisuje wiadomość żądania przed wysłaniem jej dalej.</p> | |
| Konto SIP 1 i 2 | Porty FXS1 i FXS2 |
| Konto SIP | Mapuje konta SIP na fizyczne porty. „0” reprezentuje port FXS1 a „1” reprezentuje port FXS2. |
| Przedłużenie | Numer kierunkowy |
| Wyświetlana nazwa | Wyświetlana nazwa dzwoniącego numeru. |
| Nazwa uwierzytelniania | Nazwa uwierzytelniania dla serwera Registrar/Proxy, zapewniona przez dostawcę VOIP. |
| Hasło | Hasło dla serwera Registrar/Proxy, zapewniona przez dostawcę VOIP. |
| Preferowany ptime | Czas wykorzystywany do cyfrowego próbkowania analogowego sygnału głosu. Domyślna wartość to 20 ms. |
| Preferowany kodek 1-6 | Wybierz pomiędzy kodekami G.711MuLaw/ALaw, G.729a, G.723.1, G.726_24/32, or GSM_AMR |

7.2 Zaawansowane ustawienia SIP

Poniższy ekran przedstawia zaawansowane ustawienia konfiguracji SIP.

The screenshot shows a web interface for SIP configuration. On the left is a navigation menu with the following items: 'Informacja o urządzeniu', 'Zaawansowana konfiguracja', 'Bezprzewodowy', 'Połączenie głosowe', 'Ustawienia podstawowe SIP', 'Zaawansowane ustawienia SIP' (highlighted in orange), 'Ustawienia debugowania SIP', 'Diagnostyka', 'Zarządzanie', 'Język', and 'użytkownik: root'. The main content area is titled 'Parametry globalne' and 'Usługodawca 0'. It contains the following settings: 'Przychodzący PSTN Call Routing:' with a dropdown menu set to 'Auto - PSTN Call switch to idle line'; 'PSTN Dialplan dla połączeń wychodzących:' with a text input field containing '911|102'. At the bottom of the main area are three orange buttons: 'Uruchom klienta SIP', 'Zatrzymaj klienta SIP', and 'Zastosuj'.

7.2.1 Parametry globalne

Ustawienia podstawowych parametrów.

This is a close-up of the 'Przychodzący PSTN Call Routing:' dropdown menu. The selected option is 'Auto - PSTN Call switch to idle line'. Below the dropdown are three orange buttons: 'Uruchom klienta SIP', 'Zatrzymaj klienta SIP', and 'Zastosuj'.

Przychodzący PSTN Call Routing: Definiuje, który telefon zadzwoni podczas przychodzącego połączenia.

This is another close-up of the 'Przychodzący PSTN Call Routing:' dropdown menu, showing the selected option 'Auto - PSTN Call switch to idle line'.

- **Auto**, gdy telefon 1 jest nieużywany, zadzwoni. Gdy telefon 1 jest zajęty, zadzwoni telefon 2.

| | | | |
|---------------------------------|--|---|---|
| Przychodzący PSTN Call Routing: | Line - PSTN Call switch to Physical Line ▼ | Physical Endpt To Route Incoming PSTN Calls To: | 0 |
|---------------------------------|--|---|---|

- **Line**, zawsze zadzwoni telefon 1 lub 2 w zależności od ustawienia w polu „Physical Endpt To Route Incoming PSTN Calls To. Wartość 0 – telefon 1, 1 – telefon 2.

PSTN Dial plan dla połączeń wychodzących: Definiuje numery ratunkowe. Do oddzielenia numerów użyj znaku „|”.

7.2.2 Usługodawca

Skonfiguruj Swoje ustawienia w zależności od Twojego dostawcy usługi.

Poniższe ustawienia opisane są w tabeli. Po wprowadzeniu ustawień kliknij przycisk Zastosuj aby zacząć korzystać z usługi.

UWAGA: Niektóre z poniższych opcji mogą być ustawione przy pomocy poleceń z klawiatury telefonu, opisanych na liście poleceń w rozdziale 7.4 Połączenia telefoniczne.

Parametry globalne **Usługodawca 0**

Połączenie głosowe - Zaawansowana konfiguracja SIP

UWAGA: Dla CallCtrl 1.10.x, ta strona wyświetla status aktywacji dla każdej funkcji
Dla CCTK 2.x, ta strona wyświetla włączony status dla każdej funkcji, nie konfigurowalnej z klawiatury

| Linia | 1 | 2 |
|---------------------------------|--------------------------|--------------------------|
| Połączenie oczekujące | <input type="checkbox"/> | <input type="checkbox"/> |
| Ilość przekazywanych połączeń | | |
| Bezwarunkowe przekierowanie | <input type="checkbox"/> | <input type="checkbox"/> |
| Przekazuj jeśli "zajęty" | <input type="checkbox"/> | <input type="checkbox"/> |
| Przekazuj kiedy "nie odpowiada" | <input type="checkbox"/> | <input type="checkbox"/> |
| MWI | <input type="checkbox"/> | <input type="checkbox"/> |
| Gorąca linia | <input type="checkbox"/> | <input type="checkbox"/> |
| Numer gorącej linii | | |
| Blokowanie połączeń anonimowych | <input type="checkbox"/> | <input type="checkbox"/> |
| Anonimowe połączenia | <input type="checkbox"/> | <input type="checkbox"/> |
| DND | <input type="checkbox"/> | <input type="checkbox"/> |

Włącz wsparcie T38

Rejestracja wygaśnięcia limitu czasu *

Rejestracja interwału ponawiania

DSCP dla SIP *:

DSCP dla RTP *:

Ustawienie przekaźnika DTMF *:

Ustawienie przekaźnika Hook Flash *:

Protokół transportu SIP*:

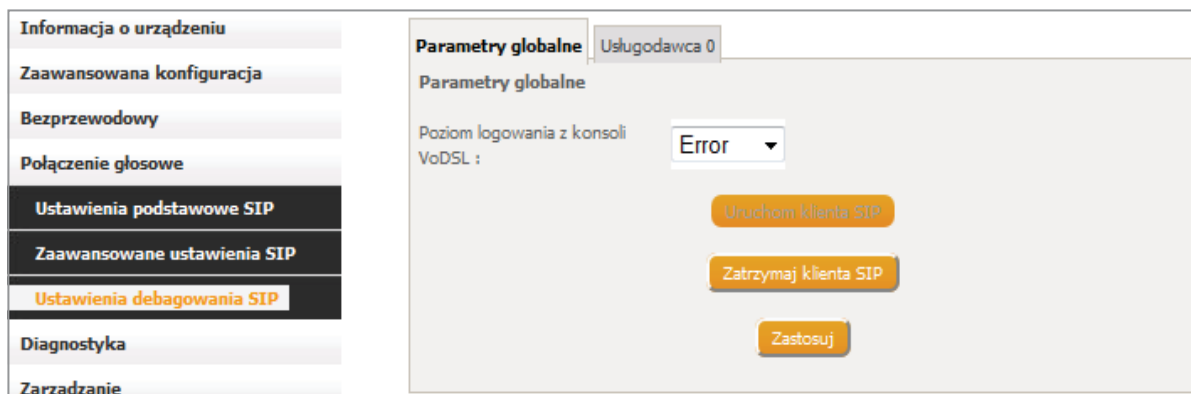
Włącz dopasowywanie tagów SIP

* Zmiana tego parametru dla jednego usługodawcy wpłynie na ustawienia wszystkich innych dostawców usług.

| Linia 1 i 2 | Porty FXS1 1 FXS2 |
|--|--|
| Połączenie oczekujące | Zaznacz pole wyboru <input type="checkbox"/> aby włączyć tę opcję. |
| Ilość przekazywanych połączeń | Numer, na który zostaną przekazane połączenia |
| Bezwarunkowe przekierowanie | Zaznacz pole wyboru <input type="checkbox"/> aby włączyć tę opcję. |
| Przekazuj jeśli "zajęty" | Zaznacz pole wyboru <input type="checkbox"/> aby włączyć tę opcję. |
| Przekazuj kiedy "nie odpowiada" | Zaznacz pole wyboru <input type="checkbox"/> aby włączyć tę opcję. |
| MWI | Włącz lub wyłącz opcję Message-Waiting Indicator (MWI) dla telefonów FXS za pomocą tego pola wyboru . |
| Blokowanie połączeń anonimowych | Zaznacz pole wyboru <input type="checkbox"/> aby włączyć tę opcję. |
| Anonimowe połączenia | Zaznacz pole wyboru <input type="checkbox"/> aby włączyć tę opcję. |
| DND (Do Not Disturb) | Zaznacz pole wyboru <input type="checkbox"/> aby włączyć tę opcję. DND (Do Not Disturb) – nie przeszkadzać |
| Włącz wsparcie T38 | Włącz lub wyłącz wsparcie dla trybu T.38 Fax za pomocą pola wyboru <input type="checkbox"/> . Możesz podłączyć fax do gniazda telefonicznego aby wysyłać i odbierać fakсы. Funkcjonalność zależy od wsparcia twojego dostawcy VoIP dla usługi Fax. |
| Rejestracja wygaśnięcia limitu czasu | Okres czasu, przez który rejestracja na serwerze Registrar/ Proxy pozostanie ważna. Domyślna wartość to 3600 s. |
| Rejestracja interwału ponawiania | Interwał czasu pomiędzy kolejnymi próbami ponownej rejestracji. |
| DSCP dla SIP | Diff Serv Code Point (DSCP) dla SIP |
| DSCP dla RTP | Diff Serv Code Point (DSCP) dla RTP |
| Ustawienie przekaźnika DTMF | Ustaw specjalne wykorzystanie pakietów RTP do przesyłu kodów DTMF. |
| Ustawienie przekaźnika Hook Flash | Przyporządkowanie zdarzenia hook flash odpowiedniemu sygnałowi. |
| Protokół transportu SIP | Ustawienie protokołu transportu wiadomości SIP |
| Włącz dopasowywanie tagów SIP (odznaczone - Vonage Interop). | Ponieważ CPE wykorzystuje tagi SIP do parowania, implementacja musi wspierać specyfikację SIP, która wymaga używania tagów. |

7.3 Ustawienia Debugowania SIP

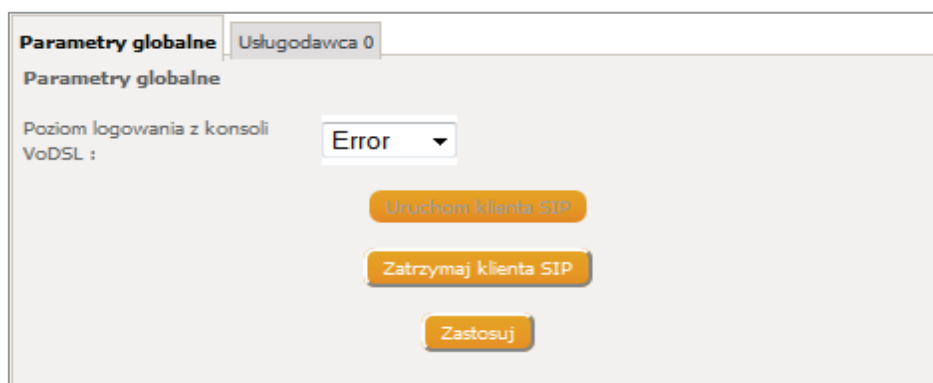
Poniższy ekran przedstawia ustawienia konfiguracji SIP wykorzystywanej do debugowania.



The screenshot shows a web interface for SIP configuration. On the left is a vertical sidebar with menu items: 'Informacja o urządzeniu', 'Zaawansowana konfiguracja', 'Bezprzewodowy', 'Połączenie głosowe', 'Ustawienia podstawowe SIP', 'Zaawansowane ustawienia SIP', 'Ustawienia debugowania SIP' (highlighted in orange), 'Diagnostyka', and 'Zarządzanie'. The main content area is titled 'Parametry globalne' and 'Usługodawca 0'. It contains a dropdown menu for 'Poziom logowania z konsoli VoDSL' set to 'Error'. Below this are three orange buttons: 'Uruchom klienta SIP', 'Zatrzymaj klienta SIP', and 'Zastosuj'.

7.3.1 Parametry globalne

Ustawienia podstawowych parametrów.



This screenshot is a zoomed-in view of the 'Parametry globalne' section. It shows the 'Poziom logowania z konsoli VoDSL' dropdown menu set to 'Error'. Below the menu are three orange buttons: 'Uruchom klienta SIP', 'Zatrzymaj klienta SIP', and 'Zastosuj'.

7.3.2 Usługodawca

Skonfiguruj Swoje ustawienia w zależności od Twojego dostawcy usługi.

Powyższe ustawienia opisane są w poniższej tabeli. Po wprowadzeniu ustawień kliknij przycisk Zastosuj aby zacząć korzystać z usługi.

| Pole wyboru <input type="checkbox"/> | Opis |
|--------------------------------------|--|
| Adres IP i Port serwera SIP log | Wprowadź adres IP i port serwera SIP log. |
| Wsparcie VAD | Zaznacz pole wyboru aby włączyć wsparcie VAD. Dostosowuje poziom wejściowy (Zysk wejściowy) i wyjściowy (Zysk wyjściowy) przy pomocy rozwijanych list. |
| Zysk wejściowy | Zwiększa poziom głośności mikrofonu (głośność z jaką jesteśmy słyszani po drugiej stronie). |
| Zysk wyjściowy | Zwiększa poziom głośności głośnika. |

7.4 Połączenia telefoniczne

Aby wykonać połączenie telefoniczne, po prostu wprowadź numer. Schemat wybierania (np. wybierane numery) jest zróżnicowany w zależności od każdej instalacji. Domyślny schemat wybierania zezwala na wybieranie 4-cyfrowych rozszerzeń numerów lub bezpośrednio adresów IP. Aby wprowadzić krótszy numer (np. 3-cyfrowy) dodaj na końcu znak „#”.

Gdy serwer połączeń (SIP Proxy Server) jest skonfigurowany w systemie, wybierane numery są tłumaczone i przekazywane przez serwer połączeń do odpowiedniego, zarejestrowanego w serwerze połączeń, odbiorcy.

Jeśli serwer połączeń nie jest skonfigurowany, połączenia nadal mogą być wykonywane przy użyciu 4-cyfrowych rozszerzeń zamiast pełnych adresów IP. Inicjator połączenia sam tłumaczy wprowadzony numer na docelowe urządzenie, jak pokazano w poniższej tabeli:

| | |
|------------------|---|
| Pierwsza cyfra: | Identyfikator linii (dla wieloliniowych bramek) |
| Pozostałe cyfry: | Numer Hosta w adresie IP. Numer sieci jest uznawany za taki sam jak adres IP dzwoniącego. |

Na przykład jeśli dzwoniący z adresu 10.136.64.33/24 wybierze numer "2023", połączenie będzie miało miejsce na drugiej linii na adresie 10.136.64.23. Wszystkie urządzenia muszą posiadać taką samą klasę C podsieci (24-bitową maskę podsieci).

Aby zadzwonić bezpośrednio na adres IP, wpisz adres IP z klawiatury, używając symbolu „*” zamiast „.” (kropki). Zakończ wpisywanie symbolem „*” lub „#”. Przy dzwonieniu za pomocą adresów IP nie ma możliwości wyboru linii na bramce, więc bramka zawsze przekieruje połączenia na pierwszą linię.

Dźwięk zajętej sieci (fast busy) będzie odegrany w przypadku nieznanymi lub nieosiągalnymi celów połączeń. Aby odebrać połączenie podnieś słuchawkę lub skorzystaj z przycisku odbierającego połączenie.

Identyfikator dzwoniącego (Caller ID)

Menadżer Połączeń przekazuje wydzwaniany numer podczas wykonywania połączeń. Wydzwaniany numer jest przesyłany na linie analogową w celu przeprowadzenia rozpoznania klas.

Zawieszanie połączenia

W celu zawieszenia połączenia, naciśnij przycisk „flash”, a następnie rozłącz się (opcjonalnie). Aby powrócić do połączenia naciśnij przycisk „flash” albo podnieś słuchawkę. Telefon przypomni Ci o zawieszonym połączeniu krótkim sygnałem dzwonka co 30 sekund.

Przekazywanie połączenia

- Aby przekazać połączenie, naciśnij przycisk „flash” a następnie wybierz numer, na który ma być przekazane połączenie.
- Aby przekazać połączenie natychmiast, rozłącz się (przekazywanie domyślne).
- Aby przekazać połączenie z konsultacją, poczekaj aż połączenie zostanie odebrane, skonsultuj i się rozłącz.
- Aby anulować przekazywanie połączenia (jeśli numer na który zostało przekazane połączenie nie odbiera); naciśnij przycisk „flash” aby powrócić do początkowego połączenia.

Połączenia konferencyjne

Aby zmienić zwykłe połączenie w połączenie konferencyjne naciśnij przycisk „flash” i wprowadź numer użytkownika, który ma dołączyć do połączenia. Poczekaj aż użytkownik odbierze połączenie i naciśnij przycisk „flash”. Aby rozłączyć dodatkowego użytkownika i powrócić do początkowego połączenia ponownie naciśnij przycisk „flash”. Aby samemu opuścić połączenie konferencyjne, rozłącz się. Połączenie zostanie przekazane (Pozostałe dwie osoby nadal będą ze sobą połączone). W trybie połączenia konferencyjnego, inicjator połączenia spełnia rolę mostka/miksera audio – ustanawiane są tylko dwa strumienie głosowe.

Połączenia oczekujące

Jeśli na linii są włączone połączenia oczekujące, i usłyszysz sygnał połączenia oczekującego podczas połączenia, naciśnij przycisk „flash” aby odebrać oczekujące połączenia. Pierwsze połączenie jest automatycznie zawieszane. Aby przełączać się między połączeniami naciśnij przycisk „flash”.

- Aby wyłączyć opcję połączeń oczekujących, wykręć na klawiaturze *60.
- Aby włączyć opcję połączeń oczekujących, wykręć na klawiaturze *61.

Opcja funkcji przekazywania połączeń (Zajęte lub Wszystkie) jest nadrzędna nad funkcją połączeń oczekujących. Funkcja połączeń oczekujących jest ignorowana jeśli przyjdzie kolejne połączenia, a jedno jest już oczekujące lub w trybie połączeń konferencyjnych.

Przekazywanie połączeń - Numer

- Aby ustawić numer, na który mają być przekazywane połączenia, wybierz na klawiaturze *74 a następnie wprowadź numer. Pamiętaj, że ustawienie tego numeru nie włącza funkcji przekazywania połączeń. Aby tego dokonać uruchom opcje przekazywania połączeń tak, jak opisano poniżej.
- Aby wyłączyć wszystkie opcje przekazywania połączeń, wybierz na klawiaturze *70.

Przekazywanie połączeń - Nie odebrane

- Aby włączyć opcję przekazywania połączeń gdy połączenie nie zostało odebrane, wybierz na klawiaturze *71. Połączenia przychodzące będą przekazywane jeśli nie zostaną odebrane w ciągu 18 sekund.

Przekazywanie połączeń - Zajęte

- Aby włączyć opcję przekazywania połączeń gdy linia jest zajęta wybierz na klawiaturze *72. Jeśli słuchawka telefonu jest podniesiona przychodzące połączenia będą natychmiast przekazywane.

Przekazywanie połączeń - Wszystkie

- Aby włączyć opcję przekazywania wszystkich połączeń wybierz na klawiaturze *73.
- Aby wyłączyć opcję przekazywania wszystkich połączeń wybierz na klawiaturze *75.

Poprzednie ustawienia „Przekazywanie połączeń – Zajęte” i „Przekazywanie połączeń - Nie odebrane” nie zostaną zmienione.

Odpowiedz na połączenie

- Aby oddzwonić na numer ostatniego, znanego przychodzącego połączenia (odebranego lub nie) wybierz na klawiaturze *69.

Wybierz ponownie

- Aby połączyć się z ostatnim wybieranym numerem wybierz na klawiaturze *68.

VoIP to PSTN

- Aby wykonać połączenie na tradycyjne telefony w sieci PSTN, wybierz najpierw na klawiaturze ##.

Rozdział 8. Diagnostyka

Pierwszy ekran Diagnostyki jest tablicą rozdzielczą, pokazującą status testów. Jeżeli test przebiegnie niepomyślnie, kliknij przycisk Test na dole tej strony, aby upewnić się, czy wynik będzie taki sam. Jeśli test ponownie przebiegnie niepomyślnie, kliknij przycisk Help i postępuj zgodnie z procedurami rozwiązywania problemów.

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|----------------------------|----------------------|----------------------|----------------------------|------|----------------------|----------------------------|------|----------------------|----------------------------|------|----------------------|--------------------------------|------|----------------------|--------------------------------------|------|----------------------|----------------------------|------|----------------------|-------------------------------------|----------|----------------------|--|----------|----------------------|---------------------------------------|----------|----------------------|---|----------|----------------------|---------------------------------|----------|----------------------|----------------------|------|----------------------|--------------------------------|------|----------------------|-------------------------|------|----------------------|
| Informacja o urządzeniu | pppoa_0_0_35 Diagnostyka Modem jest w stanie przetestować Twoje połączenie DSL. Poniżej znajdują się poszczególne testy. Jeżeli test przebiegnie niepomyślnie, kliknij przycisk "Uruchom ponownie testy diagnostyczne" na dole tej strony, aby upewnić się, czy wynik będzie taki sam. Jeśli test ponownie przebiegnie niepomyślnie, kliknij przycisk "Pomoc" i postępuj zgodnie z procedurami rozwiązywania problemów. Przetestuj połączenie z siecią lokalną <table border="1"><tr><td>Przetestuj połączenie 1X :</td><td>PASS</td><td>Help</td></tr><tr><td>Przetestuj połączenie 2X :</td><td>FAIL</td><td>Help</td></tr><tr><td>Przetestuj połączenie 3X :</td><td>FAIL</td><td>Help</td></tr><tr><td>Przetestuj połączenie 4X :</td><td>FAIL</td><td>Help</td></tr><tr><td>Przetestuj połączenie ETHWAN :</td><td>FAIL</td><td>Help</td></tr><tr><td>Przetestuj połączenie bezprzewodowe:</td><td>PASS</td><td>Help</td></tr></table> Przetestuj połączenie z dostawcą usługi DSL <table border="1"><tr><td>Test ADSL Synchronization:</td><td>FAIL</td><td>Help</td></tr><tr><td>Przetestuj ATM OAM F5 segment ping:</td><td>DISABLED</td><td>Help</td></tr><tr><td>Przetestuj ATM OAM F5 end-to-end ping:</td><td>DISABLED</td><td>Help</td></tr></table> Przetestuj połączenie z dostawcą usług internetowych <table border="1"><tr><td>Przetestuj połączenie z serwerem PPP:</td><td>DISABLED</td><td>Help</td></tr><tr><td>Przetestuj uwierzytelnianie za pomocą dostawcy usług internetowych:</td><td>DISABLED</td><td>Help</td></tr><tr><td>Przetestuj przypisany adres IP:</td><td>DISABLED</td><td>Help</td></tr><tr><td>Brama domyślna ping:</td><td>FAIL</td><td>Help</td></tr><tr><td>Ping podstawowego serwera DNS:</td><td>FAIL</td><td>Help</td></tr><tr><td>Przetestuj IP Loopback:</td><td>PASS</td><td>Help</td></tr></table> | Przetestuj połączenie 1X : | PASS | Help | Przetestuj połączenie 2X : | FAIL | Help | Przetestuj połączenie 3X : | FAIL | Help | Przetestuj połączenie 4X : | FAIL | Help | Przetestuj połączenie ETHWAN : | FAIL | Help | Przetestuj połączenie bezprzewodowe: | PASS | Help | Test ADSL Synchronization: | FAIL | Help | Przetestuj ATM OAM F5 segment ping: | DISABLED | Help | Przetestuj ATM OAM F5 end-to-end ping: | DISABLED | Help | Przetestuj połączenie z serwerem PPP: | DISABLED | Help | Przetestuj uwierzytelnianie za pomocą dostawcy usług internetowych: | DISABLED | Help | Przetestuj przypisany adres IP: | DISABLED | Help | Brama domyślna ping: | FAIL | Help | Ping podstawowego serwera DNS: | FAIL | Help | Przetestuj IP Loopback: | PASS | Help |
| Przetestuj połączenie 1X : | | PASS | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przetestuj połączenie 2X : | | FAIL | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przetestuj połączenie 3X : | | FAIL | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przetestuj połączenie 4X : | | FAIL | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przetestuj połączenie ETHWAN : | | FAIL | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przetestuj połączenie bezprzewodowe: | | PASS | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Test ADSL Synchronization: | | FAIL | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przetestuj ATM OAM F5 segment ping: | | DISABLED | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przetestuj ATM OAM F5 end-to-end ping: | | DISABLED | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przetestuj połączenie z serwerem PPP: | DISABLED | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przetestuj uwierzytelnianie za pomocą dostawcy usług internetowych: | DISABLED | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przetestuj przypisany adres IP: | DISABLED | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Brama domyślna ping: | FAIL | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Ping podstawowego serwera DNS: | FAIL | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Przetestuj IP Loopback: | PASS | Help | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Zaawansowana konfiguracja | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Bezprzewodowy | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Połączenie głosowe | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Diagnostyka | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Diagnostyka | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Zarządzanie błędami | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Zarządzanie | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Język | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| użytkownik: root | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Następne połączenie
Test Przetestuj za pomocą OAM F4

Rozdział 9. Zarządzanie

9.1 Ustawienia

9.1.1 Przywróć ustawienia domyślne

Aby przywrócić ustawienia fabryczne routera kliknij przycisk **Przywróć ustawienia domyślne**.



Po kliknięciu przycisku **Przywróć ustawienia domyślne** pojawi się poniższy ekran.

Przywracanie ustawień routera szerokopasmowego

Konfiguracja routera szerokopasmowego została przywrócona do ustawień domyślnych i router uruchamia się ponownie.

Zamknij okno konfiguracji routera szerokopasmowego i odczekaj 2 minuty przed ponownym otwarciem przeglądarki internetowej. Jeśli to konieczne, przekonfiguruj adres IP swojego komputera, aby pasował do nowej konfiguracji.

Zamknij przeglądarkę i odczekaj 2 minuty zanim powtórnie ją otworzysz. Możliwe, że będziesz musiał zmienić konfigurację IP swojego komputera aby znowu skomunikować się z routerem.

UWAGA 1: Powyższy proces ma takie samo działanie jak przycisk Reset na obudowie routera. Należy przytrzymać go przez 5 do 10 sekund, aż dioda LED zasilania będzie migać.

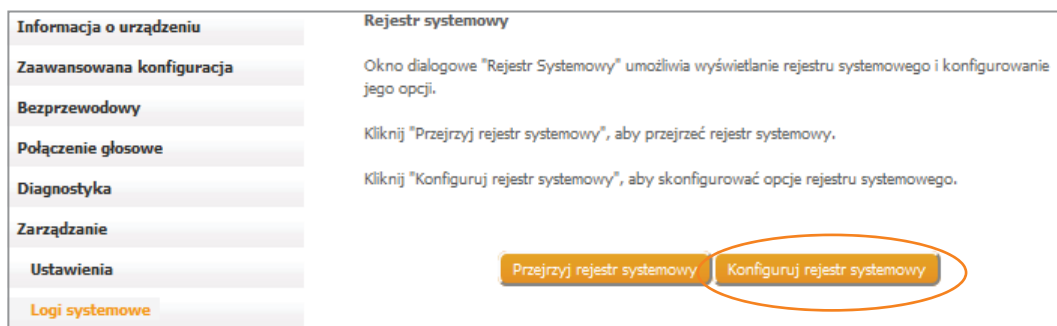
UWAGA 2: Jeśli przycisk zostanie wciśnięty przez powyżej 20 sekund router VI-3223u zostanie zablokowany (dioda Power świeci się na kolor czerwony). Przed resetem modemu należy skontaktować się z obsługą techniczną.

9.2 Logi systemowe

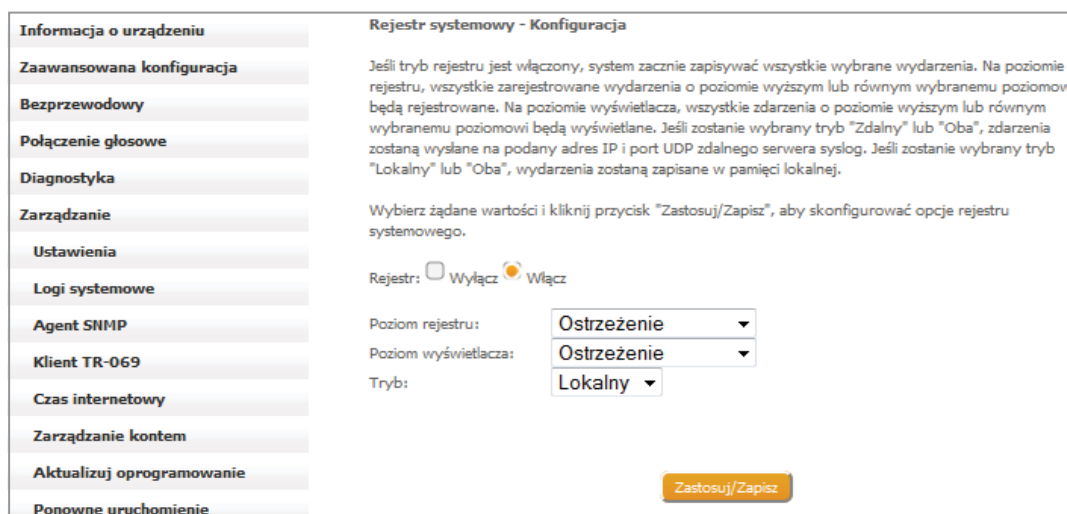
Funkcja ta pozwala zachowywać logi systemowe i przeglądać je w wybranym momencie.

Wykonaj poniższe kroki aby skonfigurować, włączyć i przeglądać logi systemowe.

KROK 1: Kliknij przycisk Konfiguruj rejestr systemowy pokazany poniżej (zakreślony na pomarańczowo).



KROK 2: Wybierz żadaną opcję i kliknij przycisk Zastosuj/Zapisz.



W poniższej tabeli przedstawiono opcje logów systemu wraz z opisami.

| Opcja | Opis |
|---------------------|---|
| Rejestr | Określa czy system zapisuje obecnie zdarzenia. Użytkownik może włączyć lub wyłączyć logowanie zdarzeń. Domyślnie logowanie jest wyłączone. Aby włączyć logowanie zaznacz pole wyboru Włącz i kliknij przycisk Zastosuj/Zapisz. |
| Poziom rejestru | <p>Pozwala na określenie poziomu zdarzeń zapisywanych i filtrowanie niechcianych zdarzeń poniżej tego poziomu. Zdarzenia od najwyższego poziomu „Awaryjny” aż do wybranego przez użytkownika będą zapisywane w buforze logu SDRAM. Kiedy bufor się wypełni, nowsze logi nadpiszą najstarsze. Domyślnie poziom rejestru ustawiony jest na „Ostrzeżenie”, który jest najniższym poziomem krytycznym.</p> <p>Poziomy rejestru zdefiniowane są następująco:</p> <ul style="list-style-type: none"> ■ Awaryjny = system nie nadaje się do użytku ■ Alert = należy podjąć natychmiastowe kroki ■ Krytyczny = warunki krytyczne ■ Błąd = warunki błędu ■ Ostrzeżenie = normalne ale niepokojące warunki ■ Powiadomienie= normalne i nieistotne warunki ■ Informacyjne= zapewnia informacje odniesienia ■ Usuwanie błędów = wiadomości usuwania błędów <p>„Awaryjny” jest najpoważniejszym poziomem, podczas gdy „Usuwanie błędów” jest najmniej ważny. Na przykład jeśli poziom rejestru zostanie ustawiony na poziomie „Usuwanie błędów”, wszystkie zdarzenia od najniższego poziomu do najwyższego „Awaryjny” zostaną zapisane. Jeśli poziom rejestru zostanie ustawiony na „Błąd”, tylko zdarzenia z tego i wyższych poziomów zostaną zapisane.</p> |
| Poziom wyświetlacza | Pozwala wybrać zdarzenia, które mają zostać wyświetlone po naciśnięciu przycisku Przejrzyj rejestr systemowy . Pokazane zostaną tylko zdarzenia z ustawionego i wyższych poziomów aż do poziomu „Awaryjny”. |
| Tryb | <p>Pozwala wybrać czy zdarzenia mają zostać zapisane lokalnie, czy wysłane do zdalnego serwera logowania, czy wykonać obydwie akcje jednocześnie. W przypadku wybrania opcji „Zdalny” przeglądanie rejestru systemowego nie będzie możliwe.</p> <p>W przypadku wyboru trybu „Zdalny” lub „Oba” WEB UI poprosi o wprowadzenie adresu IP i portu UDP serwera logowania.</p> |

Krok 3: Kliknij przycisk Przejrzyj rejestr systemowy. Wynik powinien być podobny do tego przedstawionego poniżej.

| System Log | | | |
|----------------|--------|----------|--|
| Data/Godzina | Obiekt | Severity | Wiadomość |
| Jan 1 00:00:11 | user | warn | kernel: bcmxtmcf: bcmxtmcf_init entry |
| Jan 1 00:00:11 | user | warn | kernel: adsl: adsl_init entry |
| Jan 1 00:00:11 | user | warn | kernel: Broadcom BCM636882 Ethernet Network Device v0.1 Jan 20 2012 11:27:45 |
| Jan 1 00:00:11 | user | warn | kernel: ETH Init: Ch:0 - 180 tx BDs at 0xa3901000 |
| Jan 1 00:00:11 | user | warn | kernel: ETH Init: Ch:0 - 960 rx BDs at 0xa28ac000 |

9.3 Zarządzanie kontem

9.3.1 Hasła

Poniższy ekran pozwala skonfigurować hasła dostępu do urządzenia:

- **user** - może uzyskać dostęp do routera, wyświetlić ustawienia konfiguracji i statystyki, jak również wykonać konfigurację funkcjonalności dotyczących sieci LAN.

Informacje o urządzeniu
Zaawansowana konfiguracja
Sieć bezprzewodowa
Połączenie głosowe
Diagnostyka
Zarządzanie
Ustawienia
Logi systemowe
Zarządzanie kontem
Hasła
Ponowne uruchomienie
Język
użytkownik: user

Kontrola dostępu - Hasła
Dostęp do routera szerokopasmowego jest kontrolowany przez trzy konta użytkownika: user.
Nazwa użytkownika "user" może uzyskać dostęp do routera szerokopasmowego, wyświetlić ustawienia konfiguracji i statystyki, jak również zaktualizować oprogramowanie routera od strony LAN.
Użyj pola poniżej aby wprowadzić maksymalnie 16 znaków i kliknij przycisk "Zastosuj / Zapisz", aby zmienić lub stworzyć hasła. Uwaga: Hasło nie może zawierać spacji.

Nazwa użytkownika: user
Stare hasło: ●●●●●●●●
Nowe hasło: ●●●●
Potwierdź hasło: ●●●●

Zastosuj/Zapisz

Kliknij przycisk **Zastosuj/Zapisz** aby kontynuować.

UWAGA 1: Hasło może się składać z maksymalnie 16 znaków.

UWAGA 2: Nie zaleca się stosowania polskich znaków oraz znaków specjalnych.

Informacje o urządzeniu
Zaawansowana konfiguracja
Sieć bezprzewodowa
Połączenie głosowe
Diagnostyka
Zarządzanie
Ustawienia
Logi systemowe
Zarządzanie kontem
Hasła
Ponowne uruchomienie
Język
użytkownik: user

Kontrola dostępu - Hasła
Dostęp do routera szerokopasmowego jest kontrolowany przez trzy konta użytkownika: user.
Nazwa użytkownika "user" może uzyskać dostęp do routera szerokopasmowego, wyświetlić ustawienia konfiguracji i statystyki, jak również zaktualizować oprogramowanie routera od strony LAN.
Użyj pola poniżej aby wprowadzić maksymalnie 16 znaków i kliknij przycisk "Zastosuj / Zapisz", aby zmienić lub stworzyć hasła. Uwaga: Hasło nie może zawierać spacji.

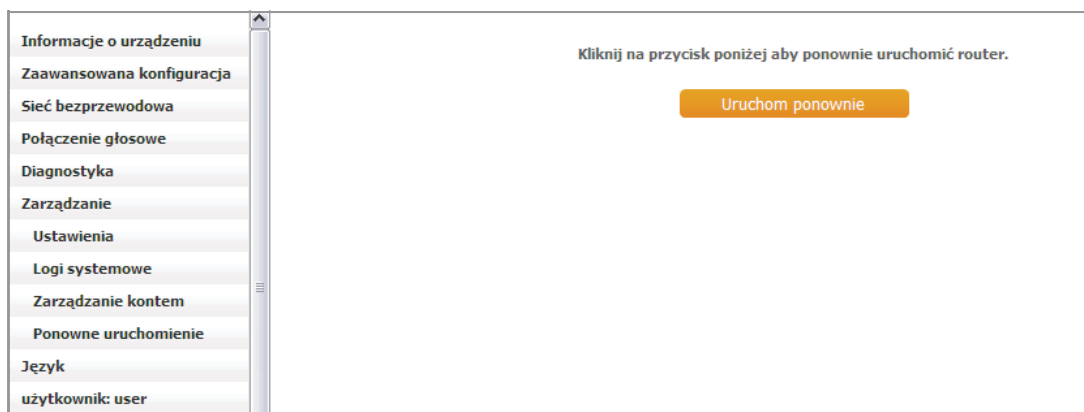
Nazwa użytkownika: user
Stare hasło: ●●●●●●●●
Nowe hasło: ●●●●
Potwierdź hasło: ●●●●

Microsoft Internet Explorer
only 0-9, A-Z, a-z is allowed in password field.
OK

9.4 Ponowne uruchomienie

Kliknij przycisk **Uruchom** ponownie aby zapisać obecną konfigurację i ponownie uruchomić router.

UWAGA: Zamknij przeglądarkę i odczekaj 2 minuty zanim powtórnie ją otworzysz. Możliwe, że będziesz musiał zmienić konfigurację IP swojego komputera aby znowu skomunikować się z routerem.



Załącznik A – Zapora sieciowa

STATEFUL PACKET INSPECTION (SPI)

Po nawiązaniu sesji przez aplikację firewall nadzoruje stan wszystkich połączeń przechodzących przez niego i analizuje nagłówki pakietów pod kątem, czy pakiety te są przesyłane przez aplikacje dopuszczone do ruchu sieciowego. W odróżnieniu od Static Packet Filtering, który analizuje pakiety tylko na podstawie informacji zawartych w ich nagłówkach.

DENIAL OF SERVICE ATTACK (DoS)

Atak polega na przeciążeniu aplikacji serwującej określone dane czy obsługującej danych klientów (np. wyczerpanie limitu wolnych gniazd dla serwerów FTP czy WWW) lub zapelnienie całego systemu plików tak, by dogrywanie kolejnych informacji nie było możliwe. Urządzenie może wytrzymać następujące ataki Dos: ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack i Tear Drop.

FILTR TCP/IP/PORT/INTERFEJSEÓW

Te reguły pomagają filtrować ruch w warstwie Sieci (warstwie 3).

Podczas tworzenia interfejsu Routowania pole **Włącz zaporę sieciową** musi być zaznaczone.

Przejdź do Zaawansowana konfiguracja → Bezpieczeństwo → Filtrowanie adresów IP.

FILTR WYCHODZĄCYCH ADRESÓW IP

Filtr ten, pomaga podczas ustanawiania reguł odrzucania pakietów interfejsu LAN. Domyślnie, jeśli Zapora sieciowa jest włączona, cały ruch adresów IP z LAN jest dozwolony. Ustanawiając jeden lub wiele filtrów, określone pakiety z LAN mogą zostać odrzucone.

| | | |
|--------------------|-------------------------|-----------------|
| Przykład 1: | Nazwa filtru | : Out_Filter1 |
| | Protokół | : TCP |
| | Źródłowy adres IP | : 192.168.1.45 |
| | Źródłowa maska podsieci | : 255.255.255.0 |
| | Port źródłowy | : 80 |
| | Docelowy adres IP | : NA |
| | Docelowy maska podsieci | : NA |
| | Port docelowy | : NA |

Powyższy filtr odrzuci wszystkie pakiety TCP pochodzące z LAN z adresu IP /maski podsieci 192.168.1.45/24 i posiadające port źródłowy 80. Wszystkie inne pakiety będą akceptowane.

| | | |
|--------------------|-------------------------|-----------------|
| Przykład 2: | Nazwa filtru | : Out_Filter2 |
| | Protokół | : UDP |
| | Źródłowy adres IP | : 192.168.1.45 |
| | Źródłowa maska podsieci | : 255.255.255.0 |
| | Port źródłowy | : 5060:6060 |
| | Docelowy adres IP | : 172.16.13.4 |
| | Docelowy maska podsieci | : 255.255.255.0 |
| | Port docelowy | : 6060:7070 |

Powyższy filtr odrzuci wszystkie pakiety UDP pochodzące z LAN z adresu IP /maski podsieci 192.168.1.45/24 i posiadające port źródłowy z zakresu od 5060 do 6060, wysyłane na adres 172.16.13.4/24 na porty z zakresu od 6060 do 7070. Wszystkie inne pakiety będą akceptowane.

FILTR PRZYCHODZĄCYCH ADRESÓW IP

Filtr ten, pomaga podczas ustanawiania reguł odrzucania i akceptowania pakietów interfejsu WAN. Domyślnie, jeśli Zapora sieciowa jest włączona, cały ruch adresów IP z WAN jest blokowany. Ustanawiając jeden lub wiele filtrów, określone pakiety z WAN mogą zostać zaakceptowane.

| | | |
|--------------------|-------------------------|------------------|
| Przykład 1: | Nazwa filtru | : In_Filter1 |
| | Protokół | : TCP |
| | Strategia | : Allow |
| | Źródłowy adres IP | : 210.168.219.45 |
| | Źródłowa maska podsieci | : 255.255.0.0 |
| | Port źródłowy | : 80 |
| | Docelowy adres IP | : NA |
| | Docelowy maska podsieci | : NA |
| | Port docelowy | : NA |
| | Interfejs WAN | : br0 |

Powyższy filtr zaakceptuje wszystkie pakiety TCP pochodzące z interfejsu WAN „br0” z adresu IP /maski podsieci 10.168.219.45/16 i posiadające port źródłowy 80. Wszystkie inne pakiety będą odrzucone.

| | | |
|--------------------|-------------------------|------------------|
| Przykład 2: | Nazwa filtru | : In_Filter2 |
| | Protokół | : UDP |
| | Strategia | : Allow |
| | Źródłowy adres IP | : 210.168.219.45 |
| | Źródłowa maska podsieci | : 255.255.0.0 |
| | Port źródłowy | : 5060:6060 |
| | Docelowy adres IP | : 192.168.1.45 |
| | Docelowy maska podsieci | : 255.255.255.0 |
| | Port docelowy | : 6060:7070 |
| | Interfejs WAN | : br0 |

Powyższy filtr zaakceptuje wszystkie pakiety UDP pochodzące z interfejsu WAN „br0” z adresu IP /maski podsieci 10.168.219.45/16 i posiadające port źródłowy z zakresu od 5060 do 6060, wysyłane na adres 192.168.1.45/24 na porty z zakresu od 6060 do 7070. Wszystkie inne pakiety będą odrzucone.

KONTROLA RODZICIELSKA

Ta opcja pozwala ograniczyć dostęp do sieci zewnętrznej wybranemu urządzeniu LAN w wybrane dni i w wybranym czasie .

| | | |
|------------------|---------------------------|---------------------|
| Przykład: | Nazwa użytkownika | : FilterJohn |
| | Adres MAC przeglądarki | : 00:25:46:78:63:21 |
| | Dni tygodnia | : pon, wt, pt |
| | Początek blokowania czasu | : 14:00 |
| | Koniec blokowania czasu | : 18:00 |

Powyższa reguła zablokuje dostęp do sieci zewnętrznej urządzeniu LAN o adresie MAC 00:25:46:78:63:21 w poniedziałki, wtorki i piątki od 14:00 do 18:00. W pozostałym przedziale czasu urządzenie będzie miało dostęp do sieci zewnętrznej.

Załącznik B - Specyfikacje

Porty zewnętrzne

1 x port RJ-11 dla ADSL2+/VDSL2,

4 x port RJ-45 dla LAN,

1 x port RJ-45 dla GigaWAN,

2 x port FXS,

1 x port FXO,

2 x port USB

przycisk Reset,

przycisk WPS,

przycisk Wi-Fi On/Off,

2 anteny Wi-Fi,

Włącznik,

WAN

Standard ADSL

ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2, AnnexM

ADSL2+

Downstream : 24 Mb/s Upstream : 1.3 Mb/s

Standard VDSL2

ITU-Y G.993.2 (wspierane profile 8a, 8b, 8c, 8d, 12a, 12b, 17a)

VDSL2

Downstream : 100 Mbps Upstream : 60 Mbps

Interfejs LAN

Standard IEEE 802.3, IEEE 802.3u

10/100 BaseT Auto-sense

MDI/MDX support Tak

Interfejs WLAN

Standard IEEE802.11n (kompatybilne z IEEE802.11b/g)

Kodowanie 64/128-bit Wired Equivalent Privacy (WEP) Kanały 11 (USA, Canada)/ 13 (Europa)/ 14 (Japonia)

Przesyłanie danych Do 300 Mb/s

WPA Tak

IEEE 802.1x Tak

WMM Tak

WPS Tak

Filtrowanie MAC Tak

Funkcje Bezpieczeństwa

Protokół uwierzytelniania: PAP, CHAP

Wyzwalanie/Przekierowanie Portów, Filtrowanie pakietów IP i adresów MAC, SSH, Kontrola Dostępu, VPN

QoS

L3 policy-based QoS, IP QoS, ToS

Usługi Głosowe

SIP RFC 3261

MGCP RFC 3435

Kodeki G.711, G.723.1, G.726, G.729ab

RTP RFC 1889

SDP RFC 2327

Caller ID zgodnie z ETSI

Echo cancellation G.168

Wycinanie ciszy: Tak

Połączenie alarmowe Tak

Zasilanie

12 Vdc / 2 A

Warunki zewnętrzne

Temperatura pracy 0 ~ 50 stopni Celsjusza

Względna wilgotność 5 ~ 95% (nie skondensowana)

Wymiary

256.2 x 166 x 47.9

Waga zestawu

(1 x VI-3223u, 1 x kabel RJ-11, 1 x kabel RJ-45, 1 x kabel USB, 1 x zasilacz, 1 x CD-ROM) = 1.1 kg

Certyfikat

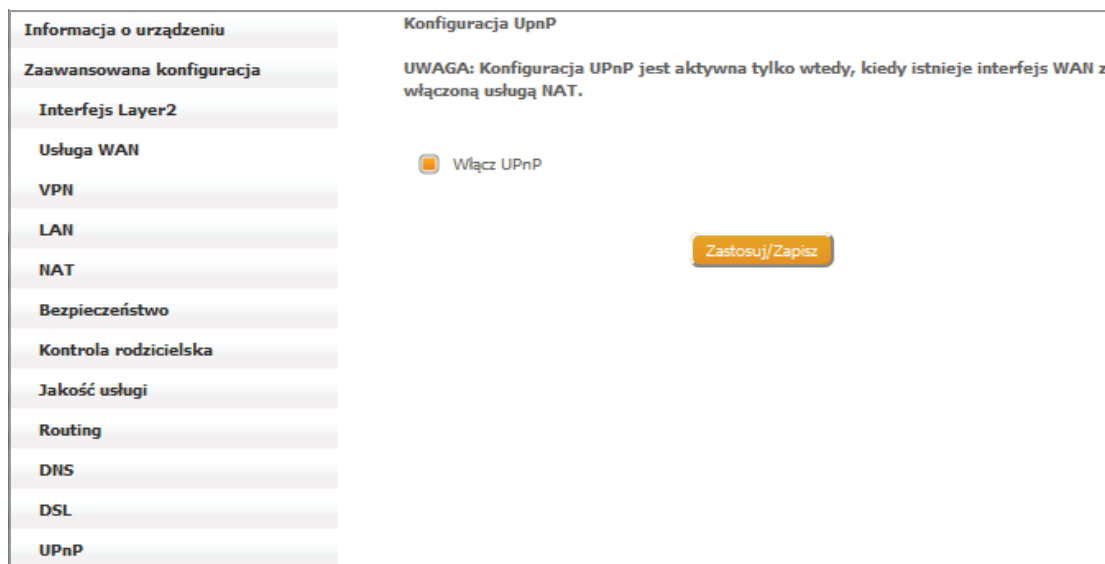
CE

UWAGA: Specyfikacja zestawu może się zmienić bez powiadomienia.

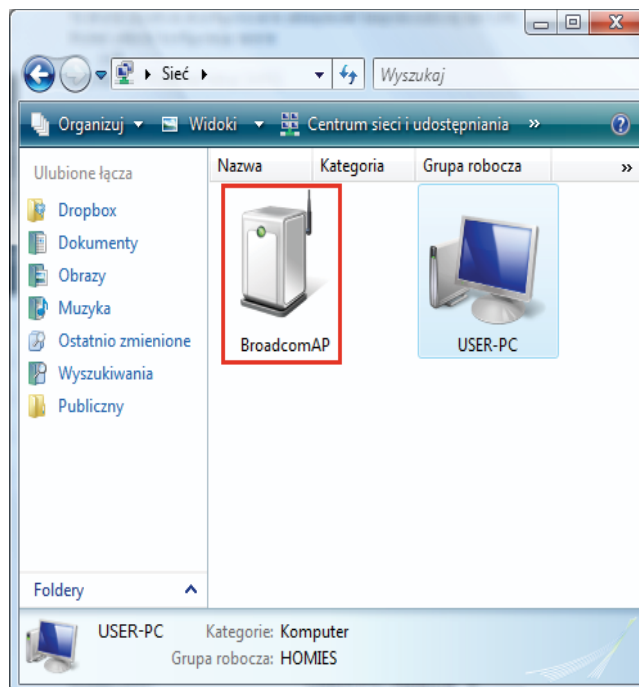
Załącznik C – Zewnętrzny Rejestrator WPS

Poniższe kroki przeprowadzą Cię przez proces dodawania external registrar za pomocą interfejsu sieciowego (Web User Interface - WUI) na Twoim komputerze z systemem Windows Vista:

KROK 1: Włącz opcję UPnP w zakładce Zaawansowana konfiguracja.



KROK 2: Na swoim komputerze otwórz folder Sieć i znajdź ikonę BroadcomAP.



KROK 3: W konfiguracji modemu, w grupie **Sieć bezprzewodowa** → zakładce **Bezpieczeństwo** włącz WPS wybierając **Enable** z rozwijanej listy i ustaw tryb WPS AP na **Unconfigured**. Kliknij przycisk **Zastosuj/Zapisz** na dole ekranu.

Komunikacja bezprzewodowa - Bezpieczeństwo

Ta strona umożliwia skonfigurowanie zabezpieczeń bezprzewodowej sieci LAN.
Możesz ustawić konfigurację ręcznie
LUB
poprzez WiFi Protected Setup (WPS)

Konfiguracja WPS

Włącz WPS Enabled ▾

Dodaj **klienta** (Ta funkcja jest dostępna tylko wtedy, gdy tryb WPA-PSK, WPA2 PSK lub tryb otwarty jest skonfigurowany)

Przycisk Wprowadź PIN STA Użyj PIN AP Dodaj Enrollee

Ustaw tryb WPS AP Unconfigured ▾

Konfiguruj AP (skonfiguruj wszystkie ustawienia zabezpieczeń z zewnętrznym rejestrem)

PIN urządzenia [Help](#)

Konfiguracja AP

Ręczna konfiguracja AP

Można ustawić metodę uwierzytelniania sieci, wybierając szyfrowanie danych.
Określ, czy klucz sieciowy jest wymagany do uwierzytelniania w sieci bezprzewodowej i określ sposób szyfrowania.
Kliknij przycisk "Zastosuj / Zapisz" po zakończeniu.

Wybierz SSID: USER-PC_Network ▾

Uwierzytelnianie sieci: WPA-PSK ▾

Hasło WPA / WAPI: [Kliknij tutaj, aby wyświetlić](#)

WPA okres odświeżania grupy klucza:

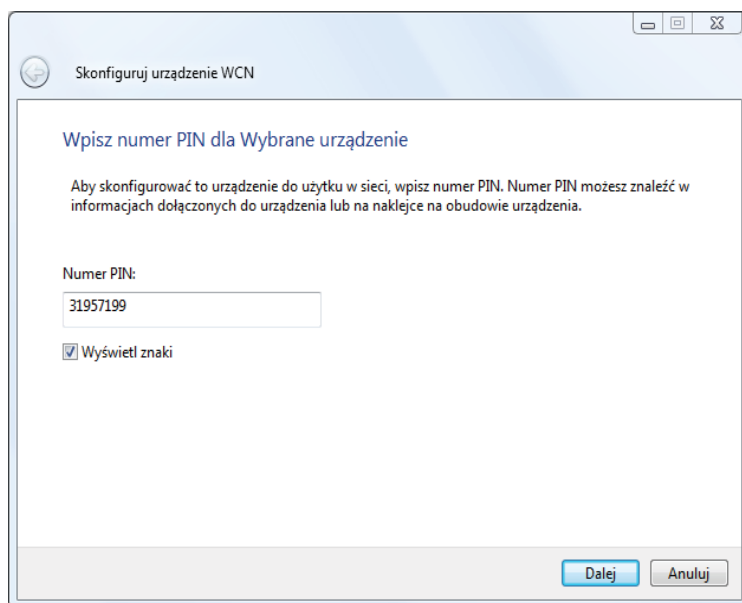
Szyfrowanie WPA / WAPI: TKIP+AES ▾

Szyfrowanie WEP: Disabled ▾

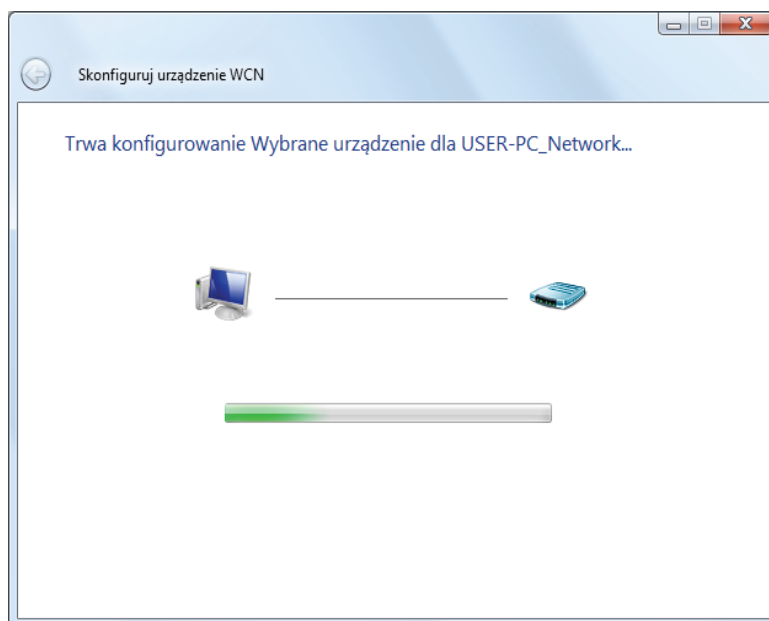
Zastosuj / Zapisz

KROK 4: Podczas akceptowania nowych ustawień bezprzewodowych router wyświetli przez chwilę pustą stronę. Kiedy powyższy ekran powróci kliknij przycisk **Konfiguracja AP** jak pokazano na powyższym ekranie.

KROK 5: Wróć do folderu Sieć na swoim komputerze i kliknij na ikonie BroadcomAP. Pojawi się okno dialogowe z pytaniem o numer PIN urządzenia. Wprowadź numer PIN taki jak pokazany na ekranie Bezprzewodowy -> Bezpieczeństwo. Kliknij przycisk **Dalej**.



KROK 6: Windows Vista podejmie próbę skonfigurowania ustawień bezpieczeństwa sieci bezprzewodowej.



KROK 7: W przypadku sukcesu, ustawienia bezpieczeństwa będą odpowiadały tym w systemie Windows Vista

Załącznik D – Serwer Wydruku

Windows XP

Poniższe kroki pokazują proces konfiguracji serwera wydruku dla systemu Windows XP.

KROK 1: Zainstaluj wymagane sterowniki Twojej drukarki. Powinny się znajdować na płycie instalacyjnej producenta drukarki.

KROK 2: Włącz **Serwer Wydruku** za pomocą interfejsu sieciowego routera w zakładce Serwer wydruku w grupie **Zaawansowana konfiguracja**.

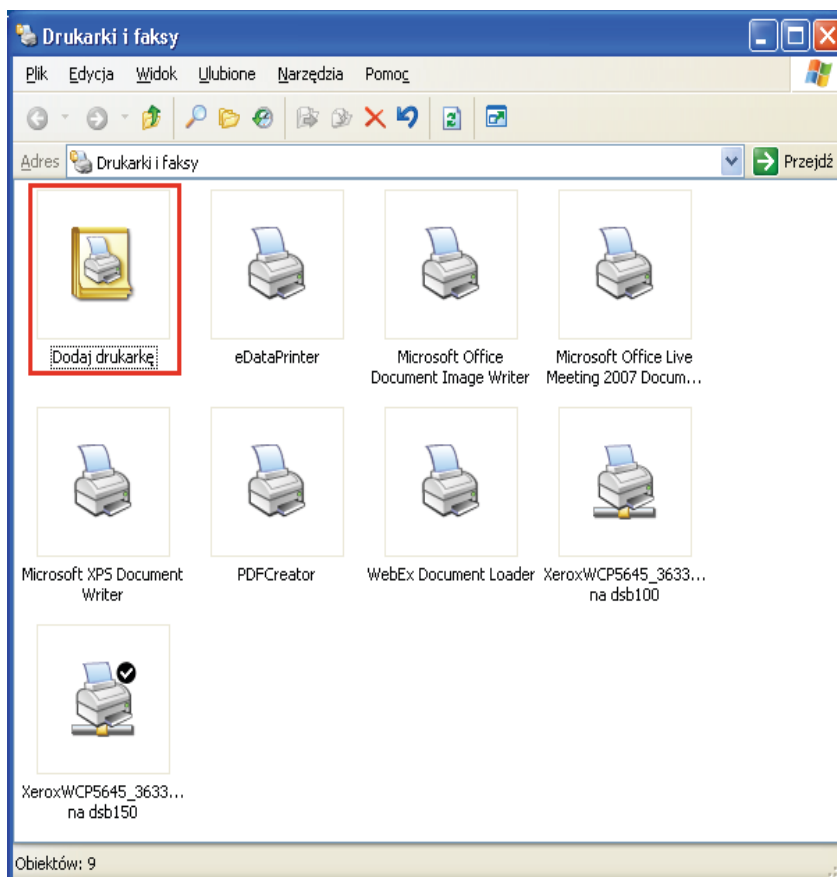
Zaznacz pole wyboru **Włącz serwer wydruku**. Wprowadź **Nazwę drukarki** oraz **Markę i model**. Następnie kliknij przycisk **Zastosuj/Zapisz**.

UWAGA: Nazwa drukarki może być dowolnym ciągiem znaków, lecz nie dłuższym niż 40 znaków.

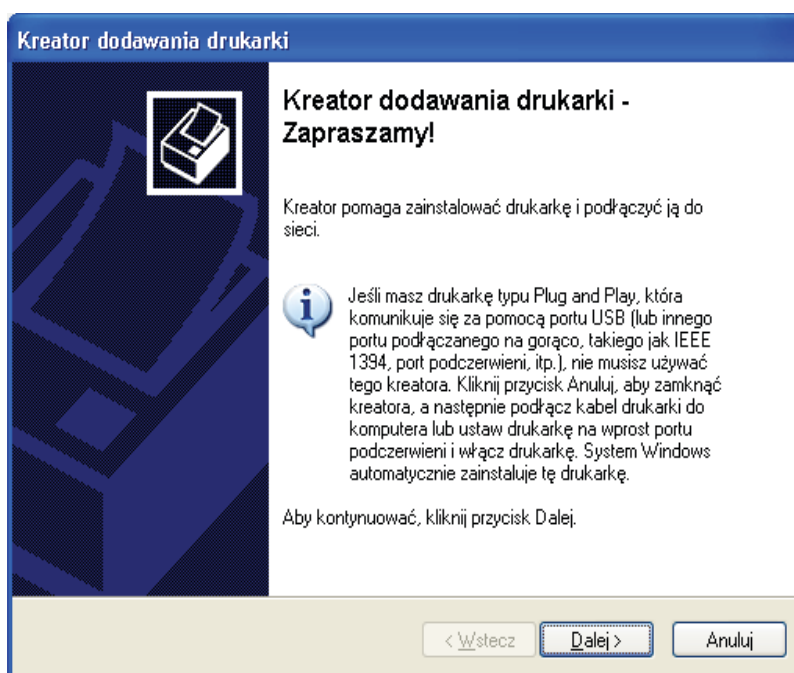
Marka i model może być dowolnym ciągiem znaków, lecz nie dłuższym niż 128 znaków.

| | |
|----------------------------------|--|
| Informacja o urządzeniu | Ustawienia serwera wydruku |
| Zaawansowana konfiguracja | Ta strona pozwala na włączenie / wyłączenie obsługi drukarki. |
| Interfejs Layer2 | <input checked="" type="checkbox"/> Włącz serwer wydruku. |
| Usługa WAN | Nazwa drukarki <input type="text" value="D2460"/> |
| VPN | Marka i model <input type="text" value="HP Deskjet D2400 Series"/> |
| LAN | <input type="button" value="Zastosuj/Zapisz"/> |
| NAT | |
| Bezpieczeństwo | |
| Kontrola rodzicielska | |
| Jakość usługi | |
| Routing | |
| DNS | |
| DSL | |
| UPnP | |
| DNS Proxy | |
| Serwer wydruku | |

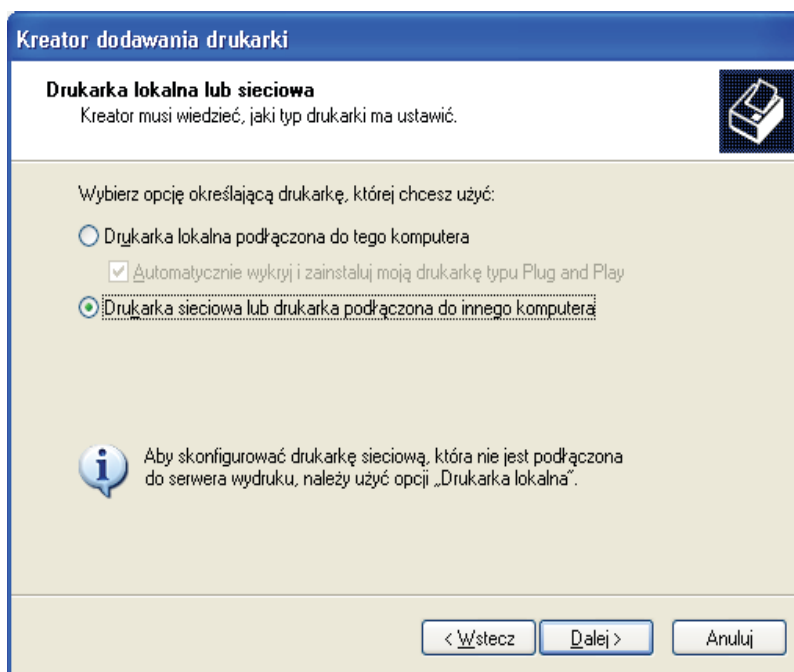
KROK 3: Przejdź do menu **Drukarki i faksy** w **Panelu sterowania** i kliknij ikonę **Dodaj drukarkę** (pokazaną na poniższym ekranie).



KROK 4: Naciśnij przycisk **Dalej** gdy pojawi się poniższe okno dialogowe.

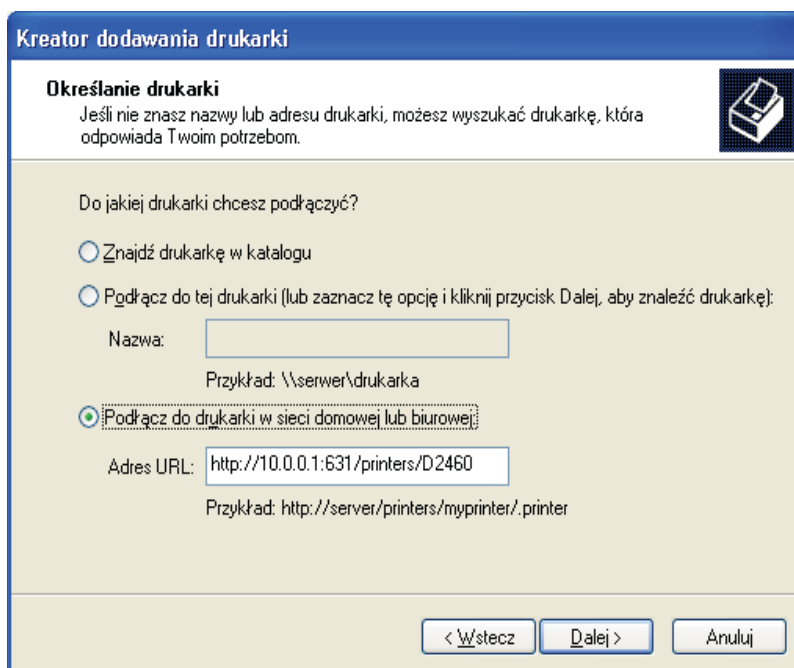


KROK 5: Wybierz pole **Drukarka sieciowa** i kliknij przycisk **Dalej**.

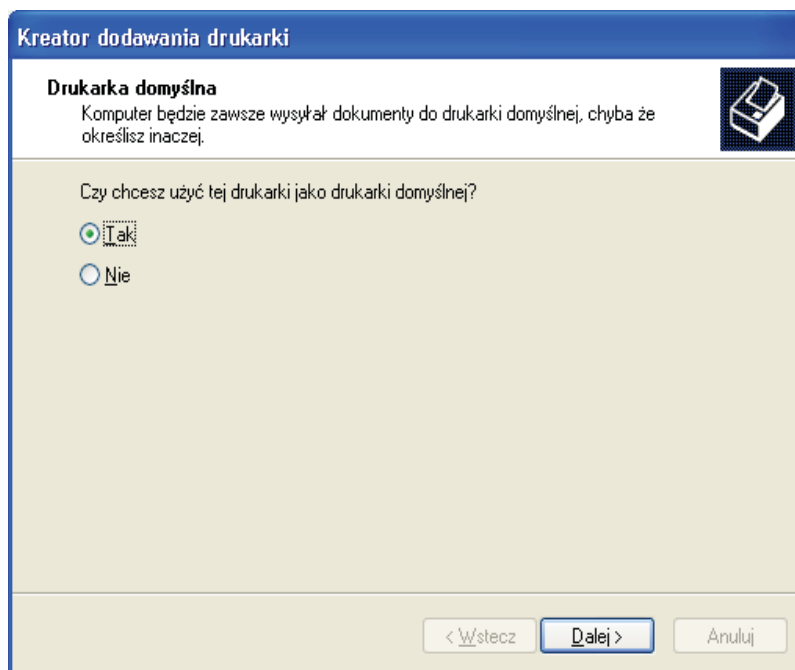


KROK 6: Wybierz pole **Podłącz do drukarki w sieci** i wprowadź link do swojej drukarki. (np. <http://10.0.0.1:631/printers/D2460>). Następnie kliknij przycisk **Dalej**.

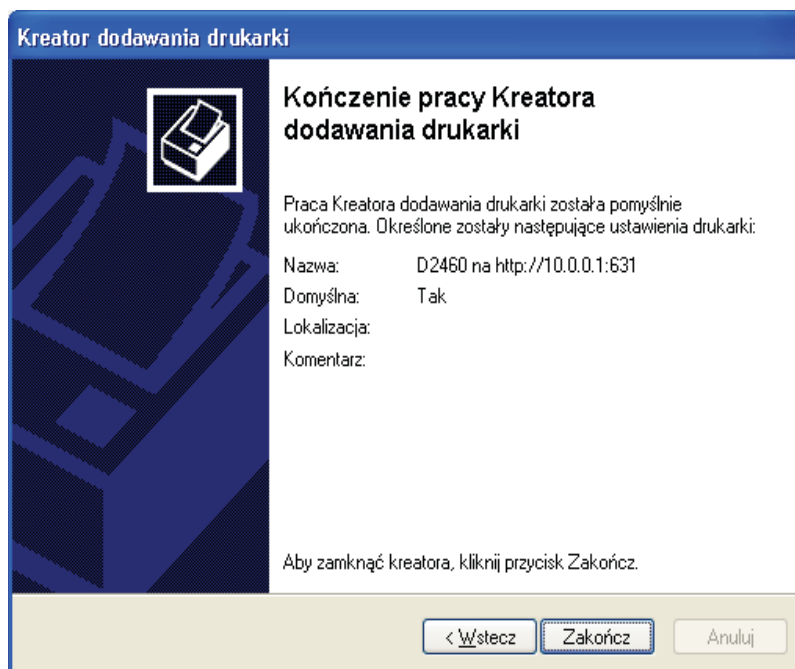
UWAGA: Nazwa drukarki musi być identyczna z tą, wprowadzoną w menu „ustawienia serwera wydruku” w kroku 2.



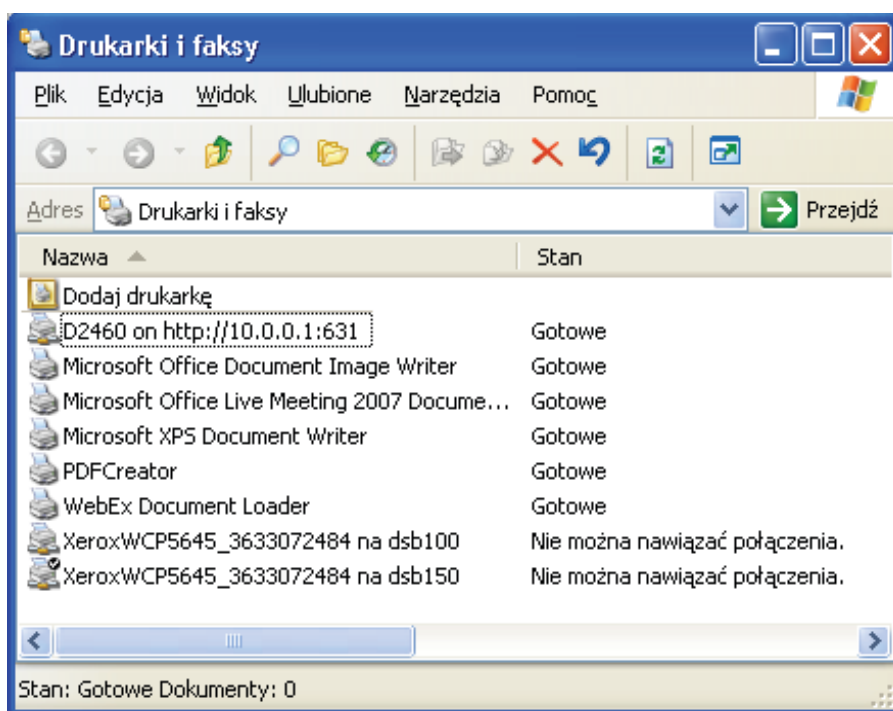
KROK 7: Wybierz **Tak** jeśli chcesz ustawić tę drukarkę jako drukarkę domyślną. W przeciwnym razie wybierz **Nie**. Kliknij przycisk **Dalej**.



KROK 8: Kliknij przycisk **Zakończ**.



KROK 9: Sprawdź stan drukarki w Panelu Sterowania w oknie Drukarki i faksy. Status powinien być widoczny jak **Gotowe**.



Windows 7

Poniższe kroki pokazują proces konfiguracji serwera wydruku dla systemu Windows 7.

KROK 1: Włącz Serwer Wydruku za pomocą interfejsu sieciowego routera w zakładce **Serwer wydruku** w grupie **Zaawansowana konfiguracja**.

Zaznacz pole wyboru **Włącz serwer wydruku**. Wprowadź **Nazwę drukarki** oraz **Markę i model**. Następnie kliknij przycisk **Zastosuj/Zapisz**.









UWAGA: Nazwa drukarki może być dowolnym ciągiem znaków, lecz nie dłuższym niż 40 znaków.

Marka i model może być dowolnym ciągiem znaków, lecz nie dłuższym niż 128 znaków.

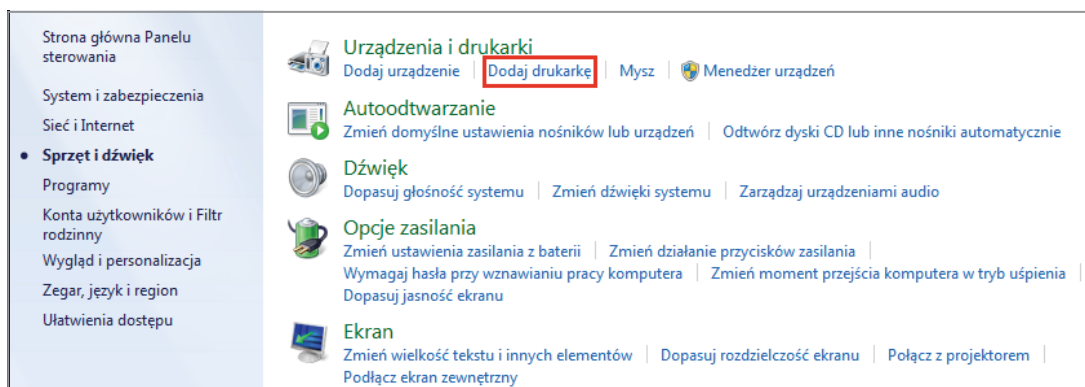
| | |
|----------------------------------|--|
| Informacja o urządzeniu | Ustawienia serwera wydruku |
| Zaawansowana konfiguracja | Ta strona pozwala na włączenie / wyłączenie obsługi drukarki. |
| Interfejs Layer2 | <input checked="" type="checkbox"/> Włącz serwer wydruku. |
| Usługa WAN | Nazwa drukarki <input type="text" value="D2460"/> |
| VPN | Marka i model <input type="text" value="HP Deskjet D2400 Series"/> |
| LAN | <input type="button" value="Zastosuj/Zapisz"/> |
| NAT | |
| Bezpieczeństwo | |
| Kontrola rodzicielska | |
| Jakość usługi | |
| Routing | |
| DNS | |
| DSL | |
| UPnP | |
| DNS Proxy | |
| Serwer wydruku | |

KROK 2: Przejdź do Panelu sterowania i kliknij ikonę Sprzęt i dźwięk.

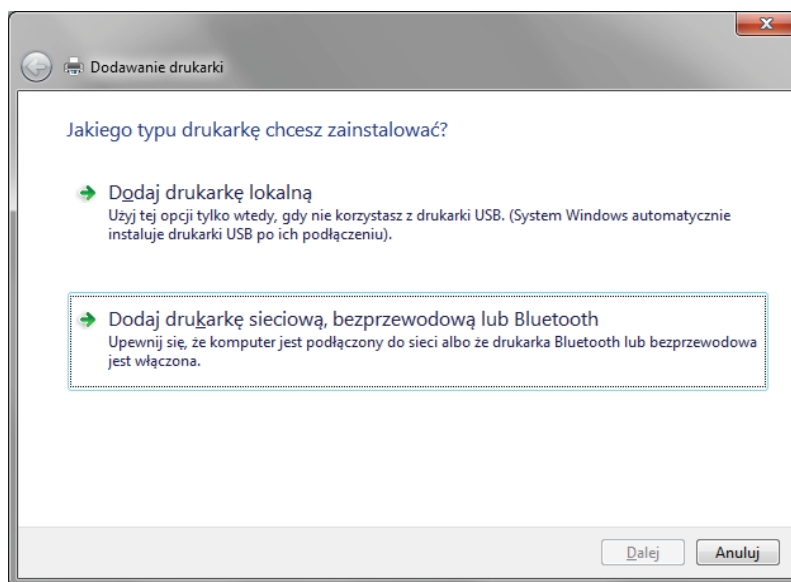
Dostosuj ustawienia komputera Widok według: **Kategoria** ▾

| | |
|--|--|
|  System i zabezpieczenia Zapoznaj się ze stanem komputera Wykonaj kopię zapasową komputera Znajdź i rozwiąż problemy |  Konta użytkowników i Filtr rodzinny Dodaj lub usuń konta użytkowników Konfiguruj ustawienia kontroli rodzicielskiej dla wszystkich użytkowników |
|  Sieć i Internet Wyświetl stan sieci i zadania Wybierz grupę domową i opcje udostępniania |  Wygląd i personalizacja Zmień kompozycję Zmień tło pulpitu Dopasuj rozdzielczość ekranu |
|  Sprzęt i dźwięk Wyświetl urządzenia i drukarki Dodaj urządzenie Połącz z projektorem Dopasuj często używane ustawienia mobilności |  Zegar, język i region Zmień klawiatury lub inne metody wprowadzania danych |
|  Programy Odinstaluj program |  Ułatwienia dostępu Niech system Windows sugeruje ustawienia Optymalizuj wyświetlacz wizualny |

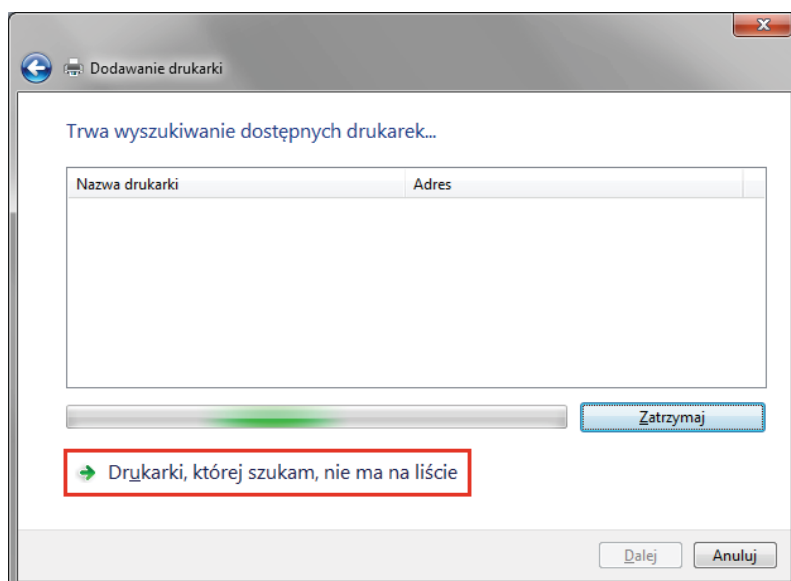
KROK 3: Kliknij pole **Dodaj drukarkę**.



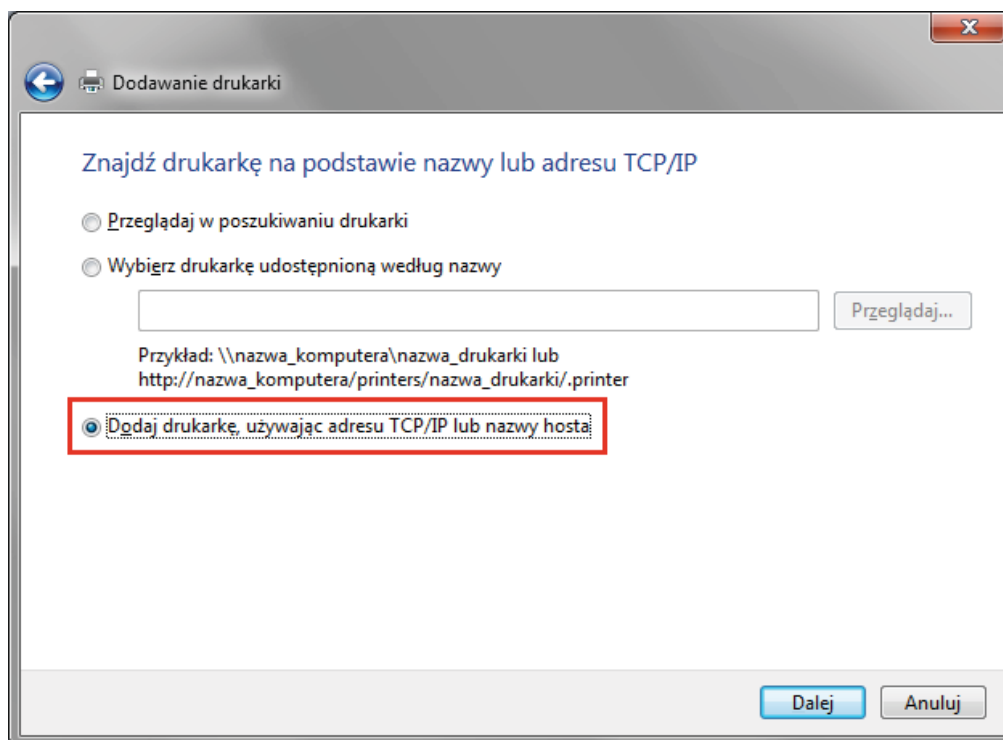
KROK 4: Wybierz pole **Dodaj drukarkę sieciową, bezprzewodową lub Bluetooth** i kliknij przycisk **Dalej**.



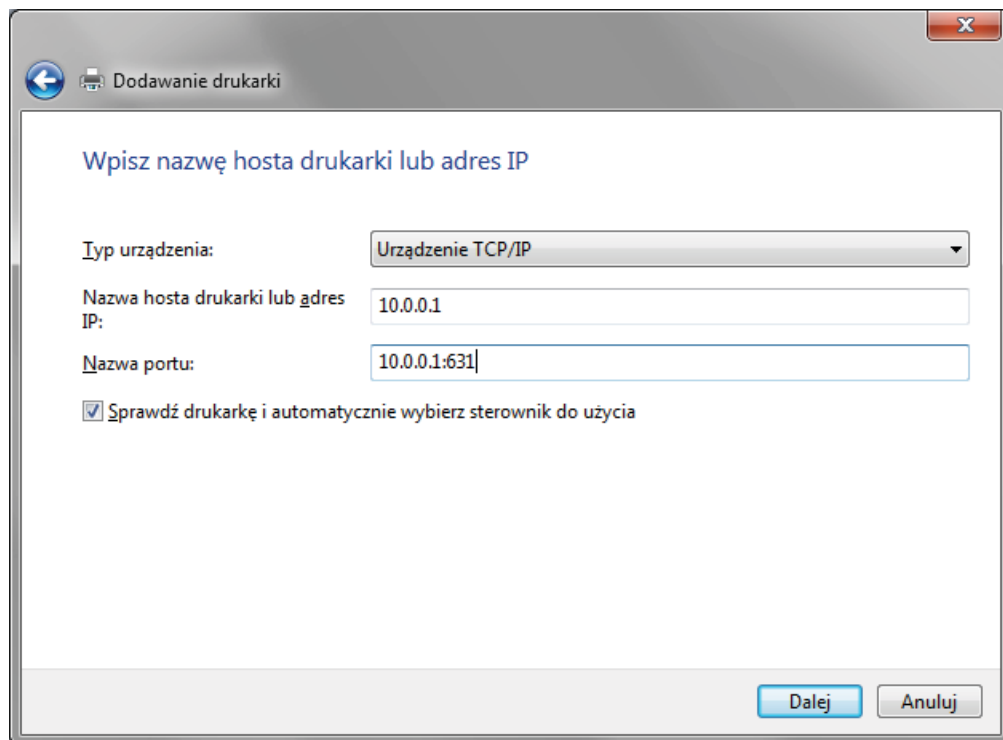
KROK 5: Kliknij pole **Drukarki, której szukam nie ma na liście**, a następnie przycisk **Dalej**.



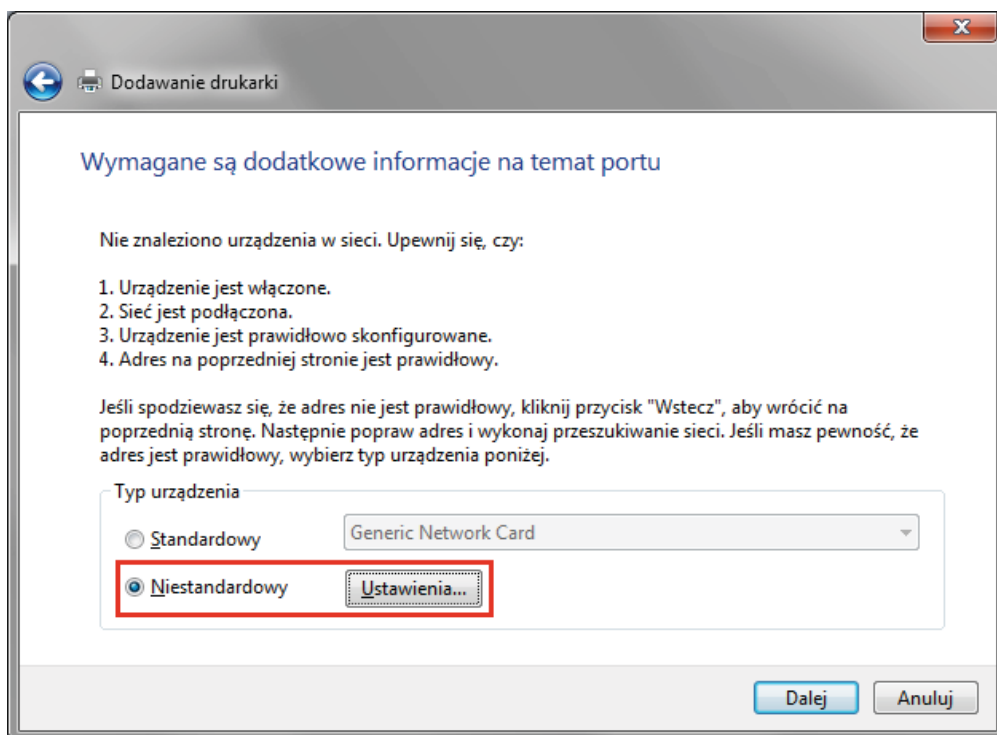
KROK 6: Zaznacz pole **Dodaj drukarkę, używając adresu TCP/IP lub nazwy hosta**, a następnie kliknij przycisk **Dalej**.



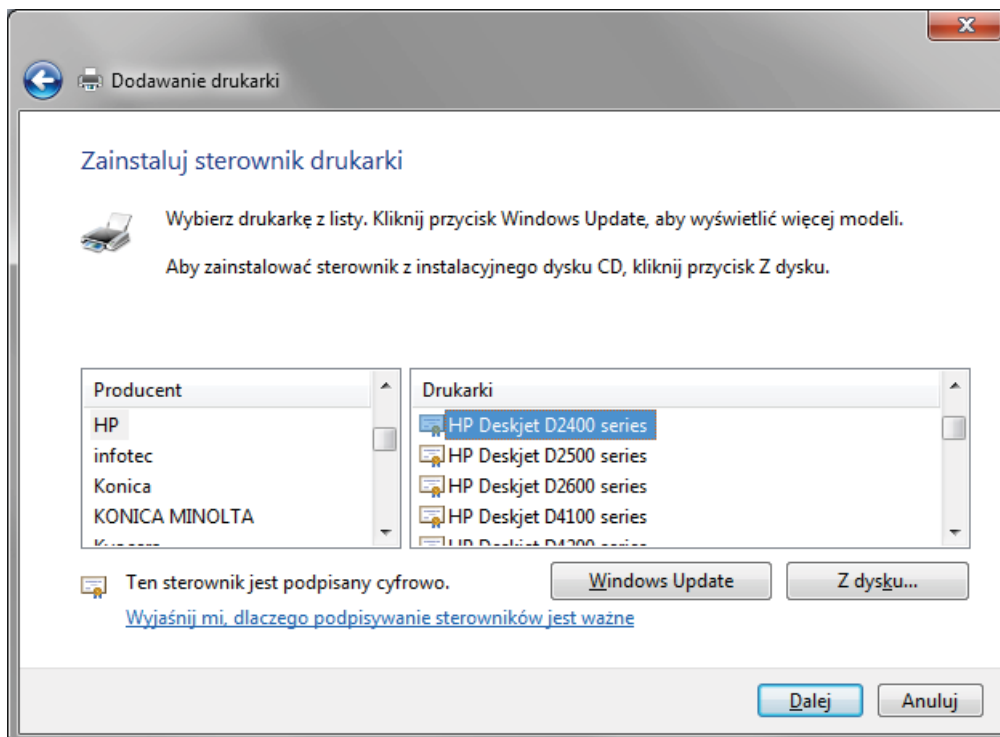
KROK 7: Wprowadź adres **10.0.0.1:631** w polu **Nazwa hosta drukarki lub adres IP** a następnie kliknij przycisk **Dalej**.



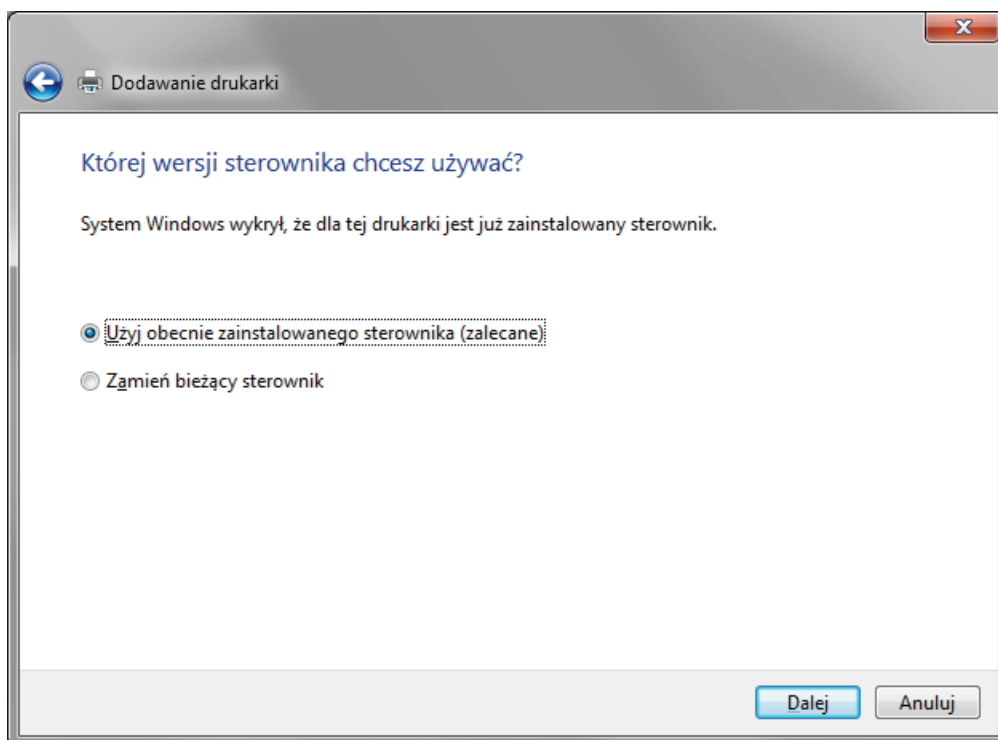
KROK 8: Zaznacz pole **Niestandardowy** a następnie kliknij przycisk **Dalej**.



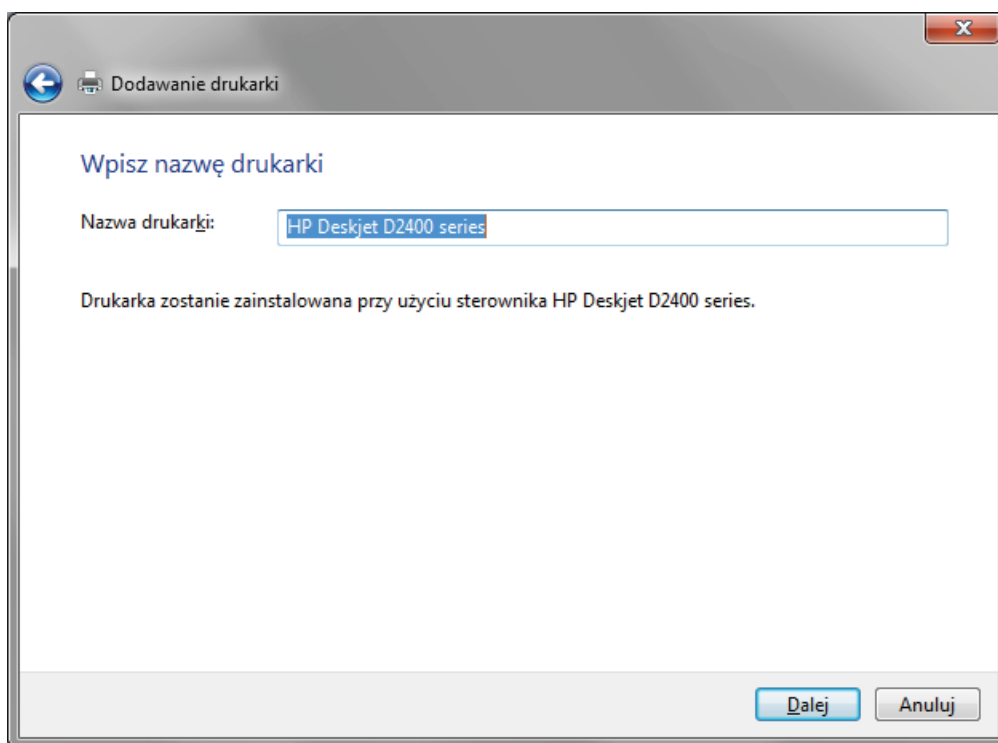
KROK 9: Wybierz swoją drukarkę z listy kliknij przycisk **Dalej**.



KROK 10: Aby kontynuować kliknij przycisk **Dalej**.



KROK 11: Wprowadź nazwę drukarki i kliknij przycisk **Dalej**.



KROK 12: Wybierz żadaną opcję i kliknij przycisk **Dalej**.

Dodawanie drukarki

Udostępnianie drukarki

Jeśli chcesz udostępnić tę drukarkę, musisz podać nazwę udziału. Możesz użyć sugerowanej nazwy lub wpisać nową. Nazwa udziału będzie widoczna dla innych użytkowników w sieci.

Nie udostępniaj tej drukarki

Udostępniaj tę drukarkę, aby inni użytkownicy w sieci mogli ją znaleźć i używać jej

Nazwa udziału:

Lokalizacja:

Komentarz:

Dalej **Anuluj**

KROK 13: Kliknij przycisk **Zakończ**.

Dodawanie drukarki

Pomyślnie dodano drukarkę HP Deskjet D2400 series.

Aby sprawdzić, czy drukarka działa prawidłowo, lub zapoznać się z informacjami o rozwiązywaniu problemów z drukarką, wydrukuj stronę testową.

Drukuj stronę testową

Zakończ **Anuluj**

Windows VISTA

Poniższe kroki pokazują proces konfiguracji serwera wydruku dla systemu Windows VISTA

UWAGA: Ta funkcja odnosi się tylko do modeli wyposażonych w port USB.

KROK 1: Włącz Serwer Wydruku za pomocą interfejsu sieciowego routera w zakładce **Serwer wydruku** w grupie **Zaawansowana konfiguracja**.

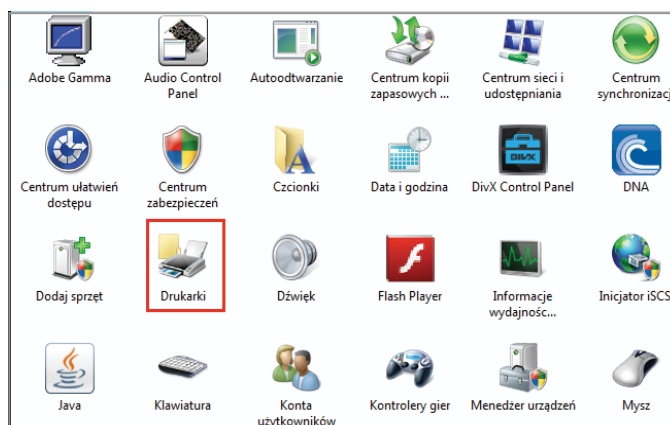
Zaznacz pole wyboru **Włącz serwer wydruku**. Wprowadź **Nazwę drukarki** oraz **Markę i model**. Następnie kliknij przycisk **Zastosuj/Zapisz**.

UWAGA: Nazwa drukarki może być dowolnym ciągiem znaków, lecz nie dłuższym niż 40 znaków.

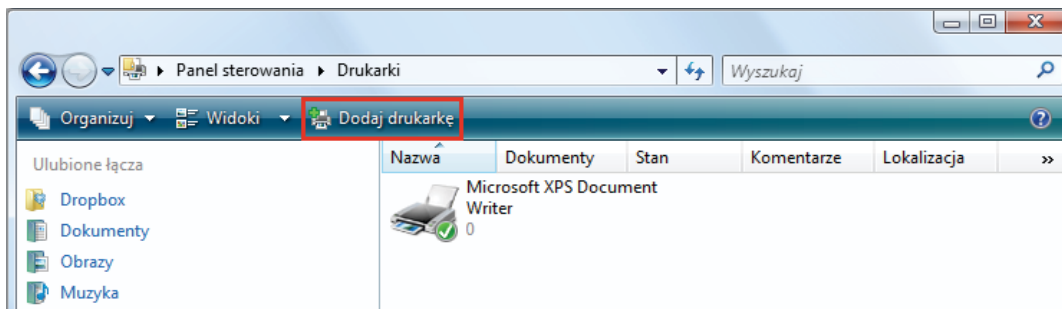
Marka i model może być dowolnym ciągiem znaków, lecz nie dłuższym niż 128 znaków.

| | |
|----------------------------------|---|
| Informacja o urządzeniu | Ustawienia serwera wydruku |
| Zaawansowana konfiguracja | Ta strona pozwala na włączenie / wyłączenie obsługi drukarki. |
| Interfejs Layer2 | <input checked="" type="checkbox"/> Włącz serwer wydruku. |
| Usługa WAN | Nazwa drukarki: D2460 |
| VPN | Marka i model: HP Deskjet D2400 Series |
| LAN | <input type="button" value="Zastosuj/Zapisz"/> |
| NAT | |
| Bezpieczeństwo | |
| Kontrola rodzicielska | |
| Jakość usługi | |
| Routing | |
| DNS | |
| DSL | |
| UPnP | |
| DNS Proxy | |

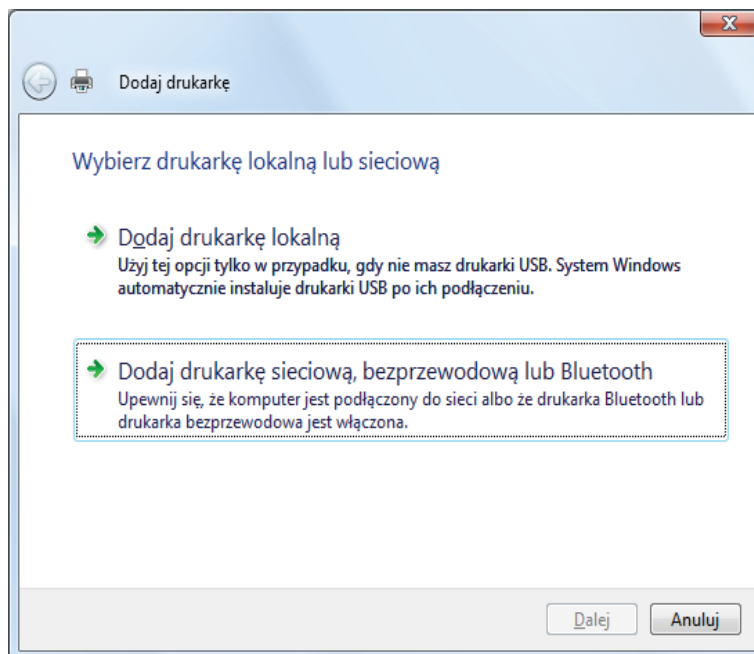
KROK 2: Przejdź do **Panelu sterowania** i kliknij ikonę **Drukarki**.



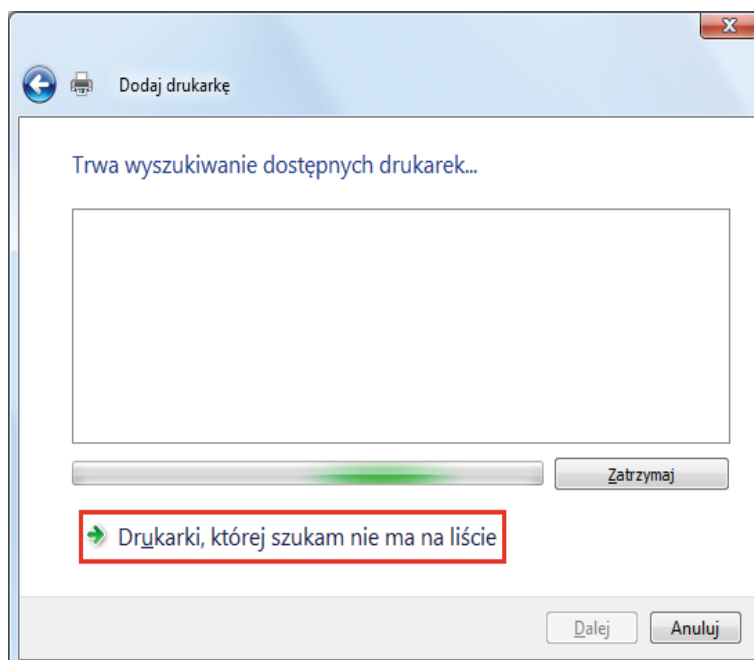
KROK 3: Kliknij pole **Dodaj drukarkę**.



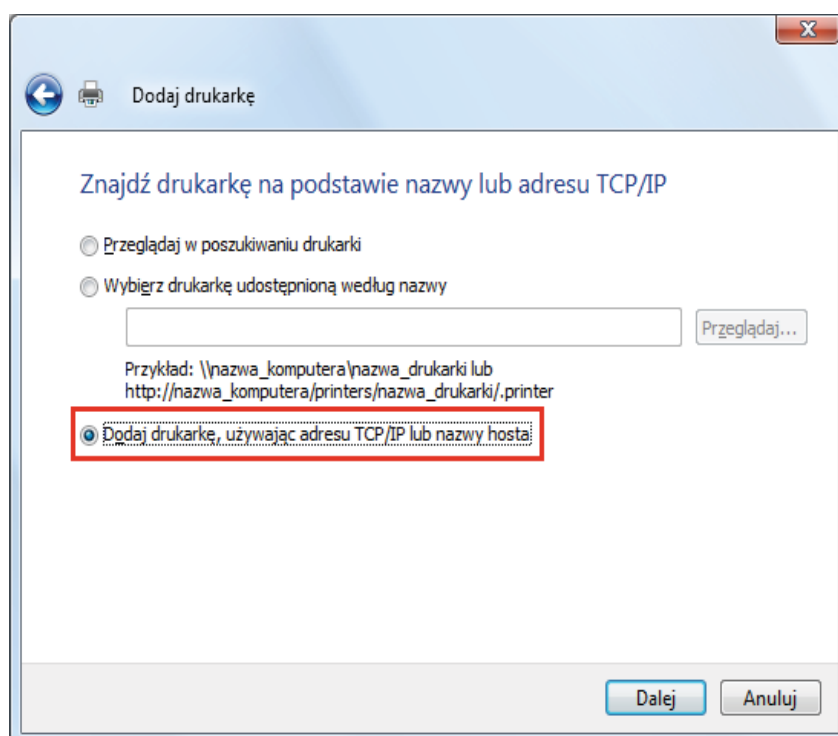
KROK 4: Wybierz pole **Dodaj drukarkę sieciową, bezprzewodową lub Bluetooth** i kliknij przycisk **Dalej**.



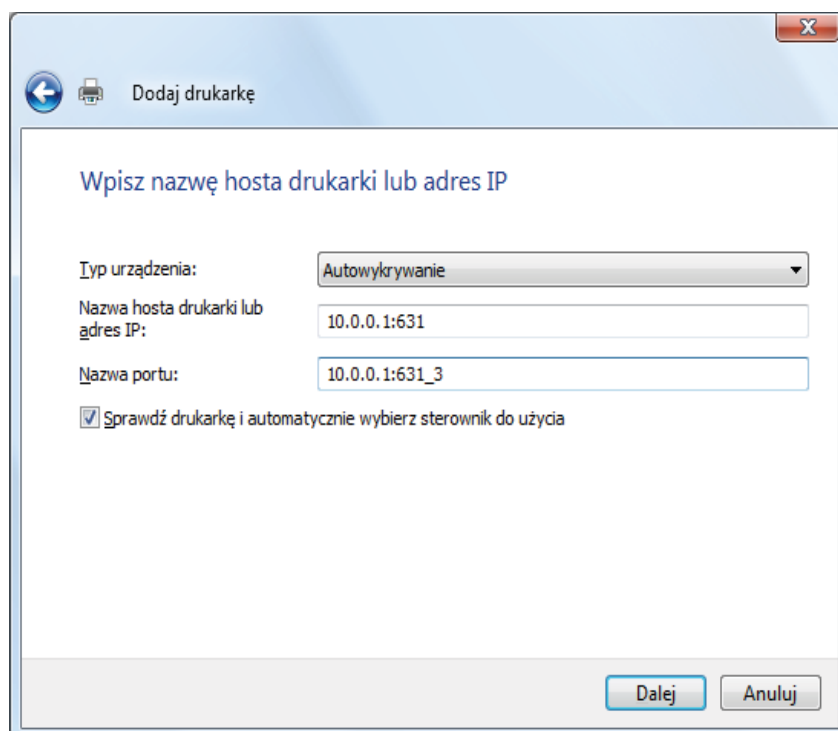
KROK 5: Kliknij pole **Drukarki, której szukam nie ma na liście**, a następnie przycisk **Dalej**.



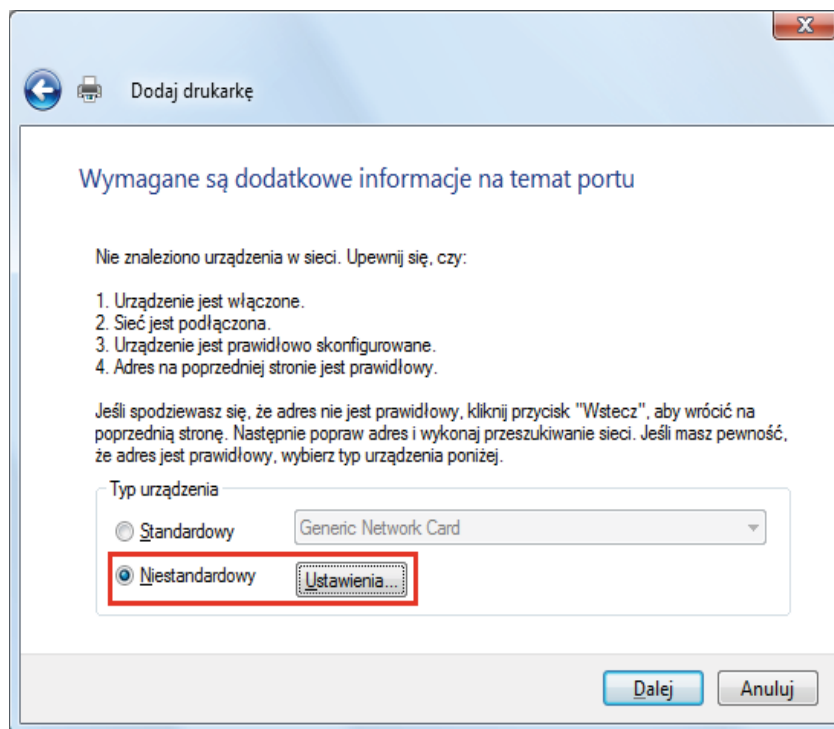
KROK 6: Zaznacz pole **Dodaj drukarkę, używając adresu TCP/IP lub nazwy hosta**, a następnie kliknij przycisk **Dalej**.



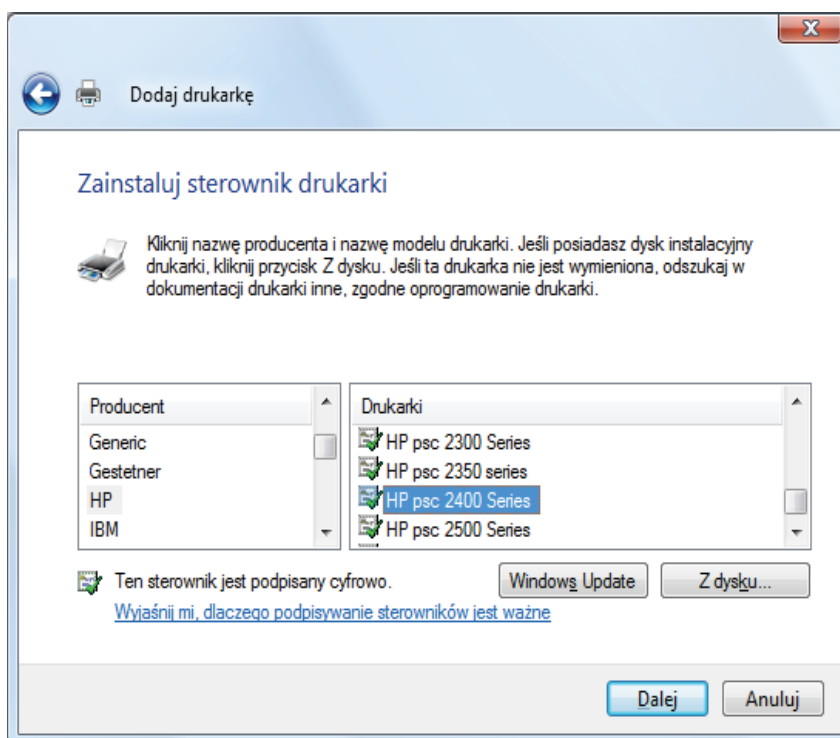
KROK 7: Wprowadź adres **10.0.0.1:631** w polu **Nazwa hosta drukarki lub adres IP**, a następnie kliknij przycisk **Dalej**.



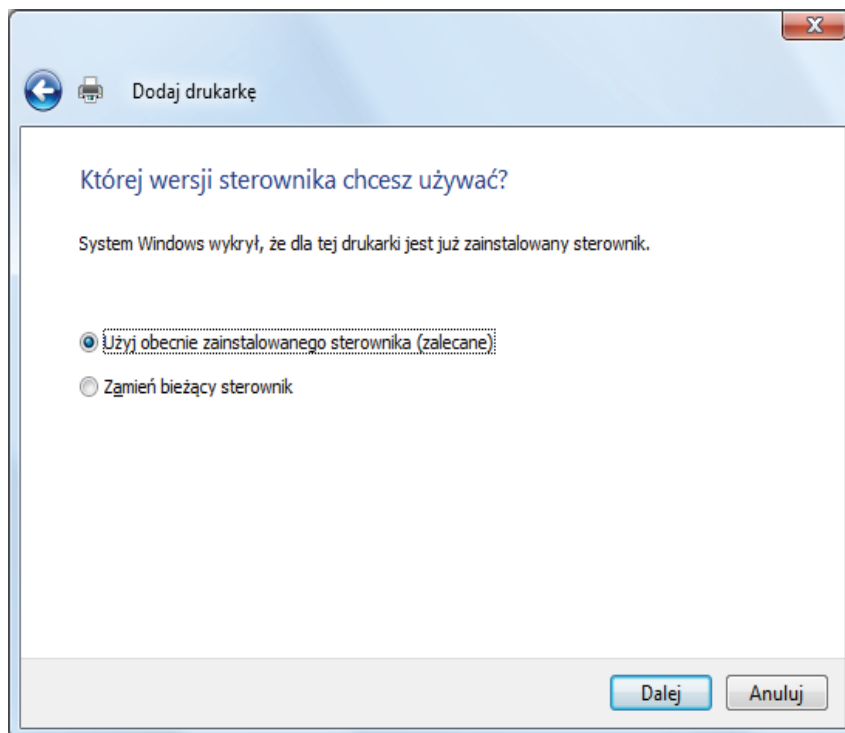
KROK 8: Zaznacz pole **Niestandardowy**, a następnie kliknij przycisk **Dalej**.



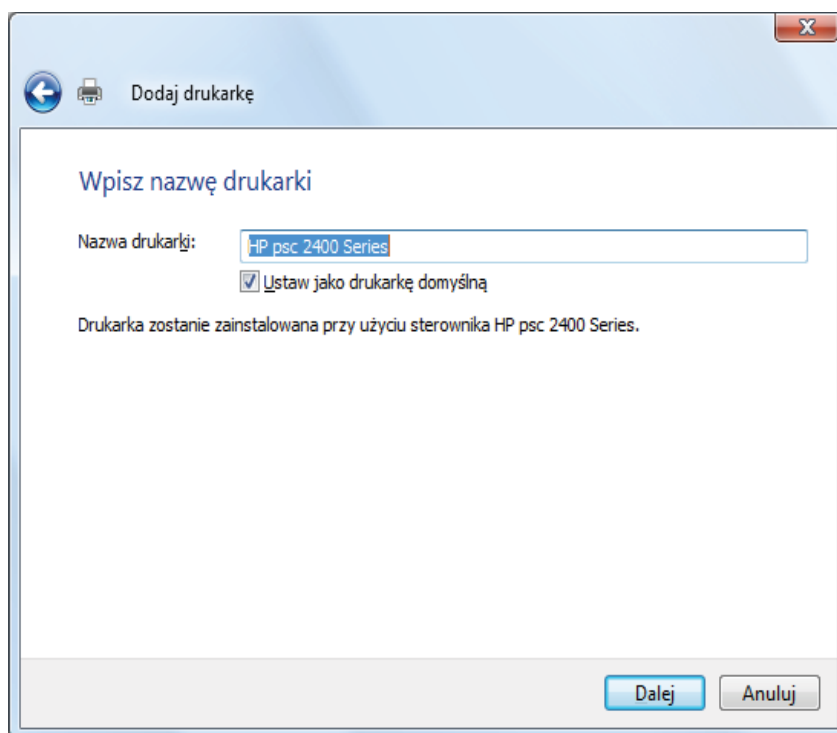
KROK 9: Wybierz swoją drukarkę z listy kliknij przycisk **Dalej**.



KROK 10: Aby kontynuować kliknij przycisk **Dalej**.



KROK 11: Wprowadź nazwę drukarki i kliknij przycisk **Dalej**.



KROK 12: Kliknij przycisk **Zakończ**.

