Netia Spot
instrukcja obsługi
panelu konfiguracyjnego

NETIA

Spis treści

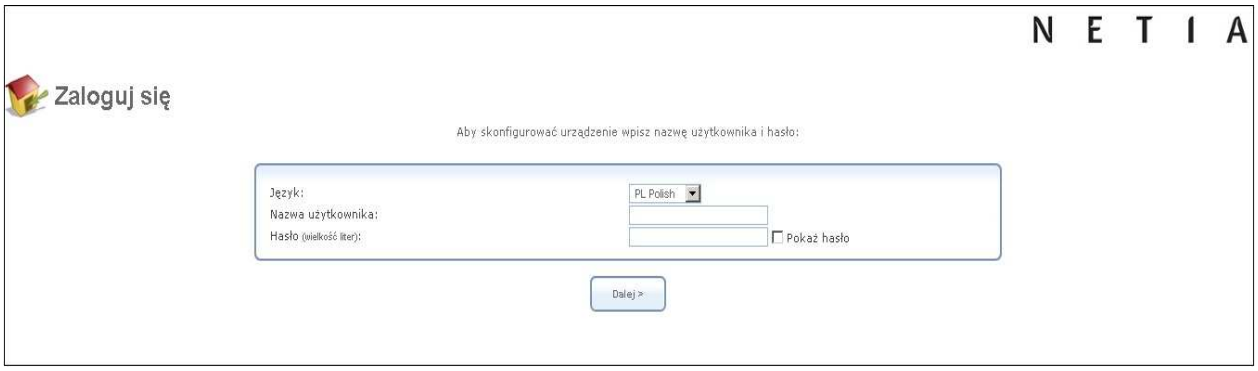
1 Dostęp do konsoli zarządzania

Ten rozdział opisuje, jak używać konsoli zarządzania OpenRG, a także podstawowy panel zarządzania (WBM), który pozwala skonfigurować i kontrolować wszystkie funkcje i parametry systemu OpenRG, za pomocą przyjaznego dla użytkownika interfejsu graficznego. Ten przyjazny dla użytkownika interfejs realizowany jest także w strukturze dokumentacji WBM, która opiera się bezpośrednio na strukturze WBM. Tutaj znajdziesz łatwo potrzebne funkcje, zarówno w interfejsie WBM, jak i jego dokumentacji.

Ważna uwaga: Ten dokument może zawierać informacje na temat funkcji i możliwości, które nie są dostępne w opisywanym urządzeniu. Pomimo dołożenia wszelkich starań podjętych w celu dostosowania niniejszej instrukcji w jak największym stopniu do urządzenia, mogą istnieć pewno różnice.

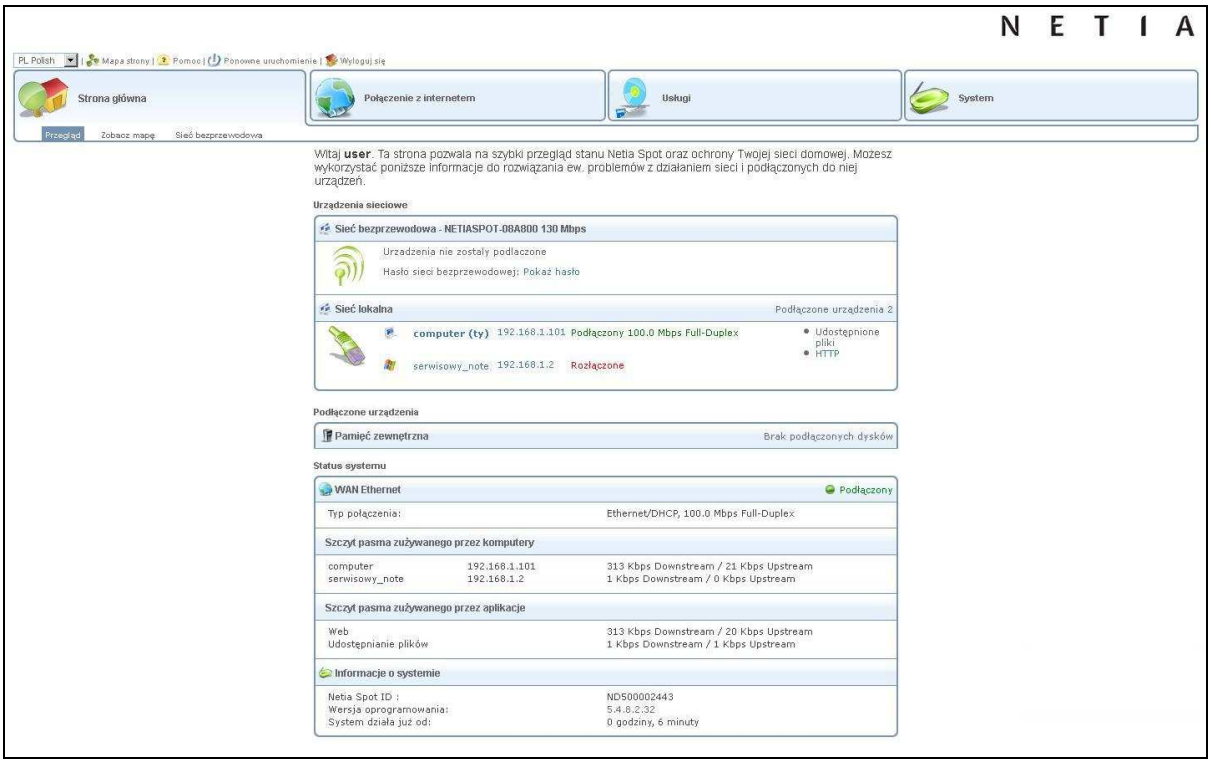
Aby uzyskać dostęp do panelu zarządzania urządzeniem:

1. Uruchom przeglądarkę internetową na komputerze w sieci LAN.
2. W pasku adresu wpisz nazwę urządzenia lub jego adres IP. Domyślna nazwa urządzenia w sieci to http://netiaspot.home, domyślny adres IP to **192.168.1.254**. Ekran logowania wygląda, jak poniżej.



Rysunek 1.1 Ustawienia logowania się do panelu konfiguracyjnego

Wprowadź swoją nazwę użytkownika i hasło, a następnie kliknij przycisk „Dalej”. Domyślna nazwa użytkownika to „user”, domyślne hasło to „user”.



Rysunek 1.2 WBM

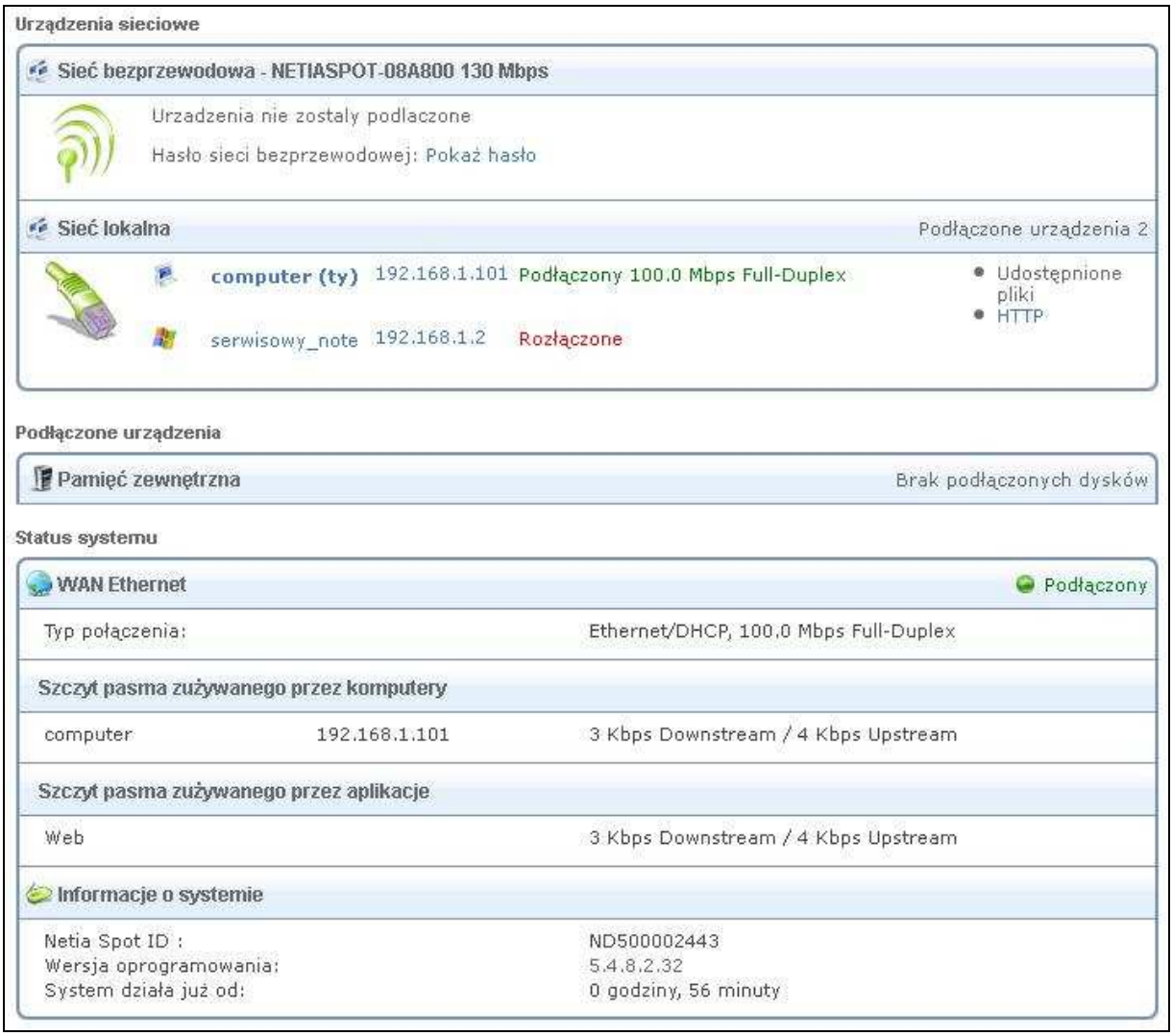
Uwaga: Możesz także zalogować się w bardziej zaawansowanym trybie administracyjnym, wpisując „**admin**” jako nazwę użytkownika, a jako hasło „**admin_netia**”. Aby się wylogować, kliknij link „Wyloguj”. Znajduje się on na górnym pasku interfejsu zarządzania.

Sesja logowania wygasa automatycznie po dłuższym okresie bezczynności. Jeśli spróbujesz wejść do panelu zarządzania po wygaśnięciu sesji, wyświetlony zostanie ponownie ekran logowania. Funkcja ta zapobiega nieautoryzowanemu dostępowi do sesji i zmianom ustawień bramy.

2 Strona główna

2.1. Przegląd urządzenia

Ekran „Przegląd" prezentuje stan różnych modułów OpenRG w jednym miejscu. Możesz szybko i sprawnie sprawdzić ważne informacje systemowe, takie jak status połączenia z internetem, status sieci bezprzewodowej, status połączenia lokalnego, jak również status urządzenia peryferyjnego.



Rysunek 2.1 Strona główna – Przegląd

2.1.1. Przeglądanie i podłączenie do nadającej sieci bezprzewodowej

Sekcja wyświetlająca „Urządzenia sieciowe" pokazuje nazwę sieci punktu bezprzewodowego OpenRG. Aby połączyć się z siecią bezprzewodową z komputera posiadającego systemem Windows, wykonaj następujące czynności:

1. W pasku zadań systemu Windows, kliknij ikonę połączenia bezprzewodowego.

Rysunek 2.2 Ikona połączenia bezprzewodowego w zasobniku systemowym

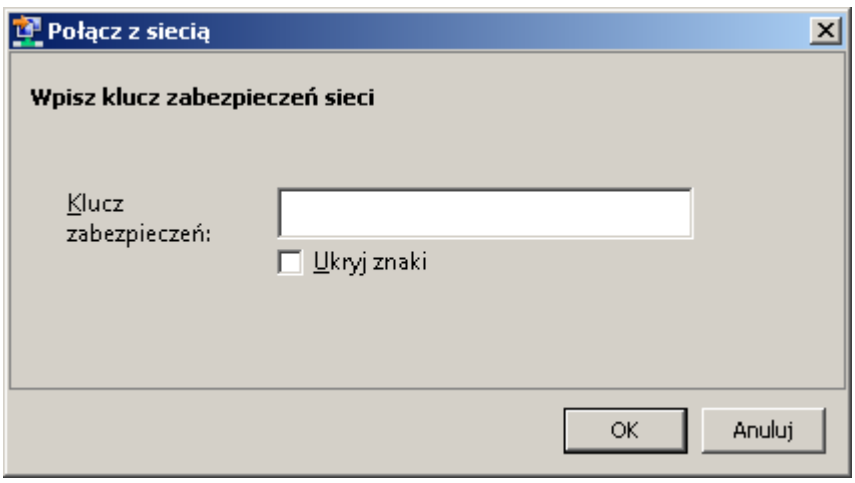
Ekran „Połączenie sieci bezprzewodowej", wyświetla wszystkie dostępne sieci bezprzewodowe (nazywane także jako Wi-Fi) w zasięgu naszego komputera. Jeżeli Twoje urządzenie Netia Spot jest podłączone i aktywne, powinieneś zobaczyć nazwę jego sieci bezprzewodowej jako widoczną w wykrytych sieciach bezprzewodowych naszego komputera. Domyślna nazwa sieci bezprzewodowej (SSID) to „NETIASPOT-XXXXXX", gdzie XXXXXX to ostatnie sześć znaków z adresu MAC urządzenia (na naklejce znajdującej się na spodzie urządzenia znajduje się wydrukowana nazwa sieci bezprzewodowej, klucz dostępowy do sieci bezprzewodowej – WPA i kod PIN, jeśli nasza karta bezprzewodowa wspiera funkcje automatycznej konfiguracji zabezpieczeń WPS).

Rysunek 2.3 Dostępne połączenia bezprzewodowe

Jeśli nie widzisz sieci, należy odświeżyć listę wykrytych sieci przy użyciu funkcji „Odśwież listę sieci".

2. Wybierz połączenie bezprzewodowe i kliknij „Połącz" na dole ekranu.

Po pojawieniu się okna, wymagającego podania hasła WPA (klucz sieciowy), należy wpisać klucz WPA.

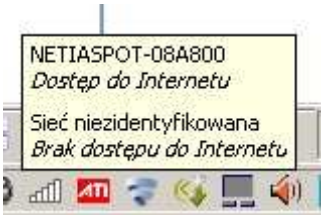


Rysunek 2.4 Klucz uwierzytelniania sieci WPA

Wprowadź hasło WPA. Wielkość liter hasła ma znaczenie. Hasło WPA można znaleźć na naklejce znajduje się w dolnej części urządzenia i może być zmienione w menu „Sieć bezprzewodowa" w zakładce „Strona główna". Po nawiązaniu połączenia, stan połączenia bezprzewodowego w naszym komputerze zmieni się na „Połączony".

Rysunek 2.5 Połączenie z siecią bezprzewodową

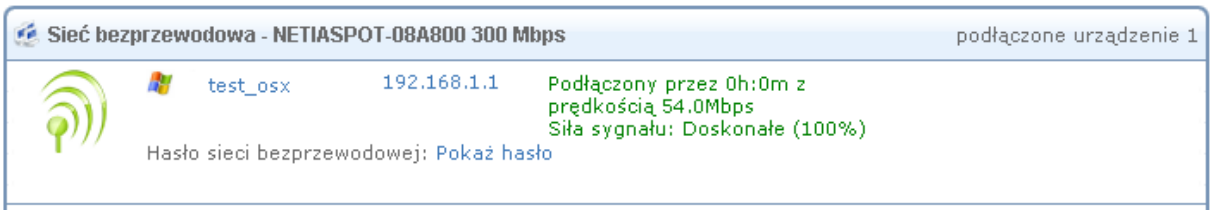
Dymek jest wyświetlany w obszarze powiadomień, oznaczając powodzenie i podłączenie do sieci bezprzewodowej.



Rysunek 2.6 Informacje o połączeniu bezprzewodowym

3. Otwórz przeglądarkę internetową i przejdź do dowolnej witryny.

Zakładka „Strona główna” wyświetla informacje o podłączonych bezprzewodowo komputerach lub urządzeniach.

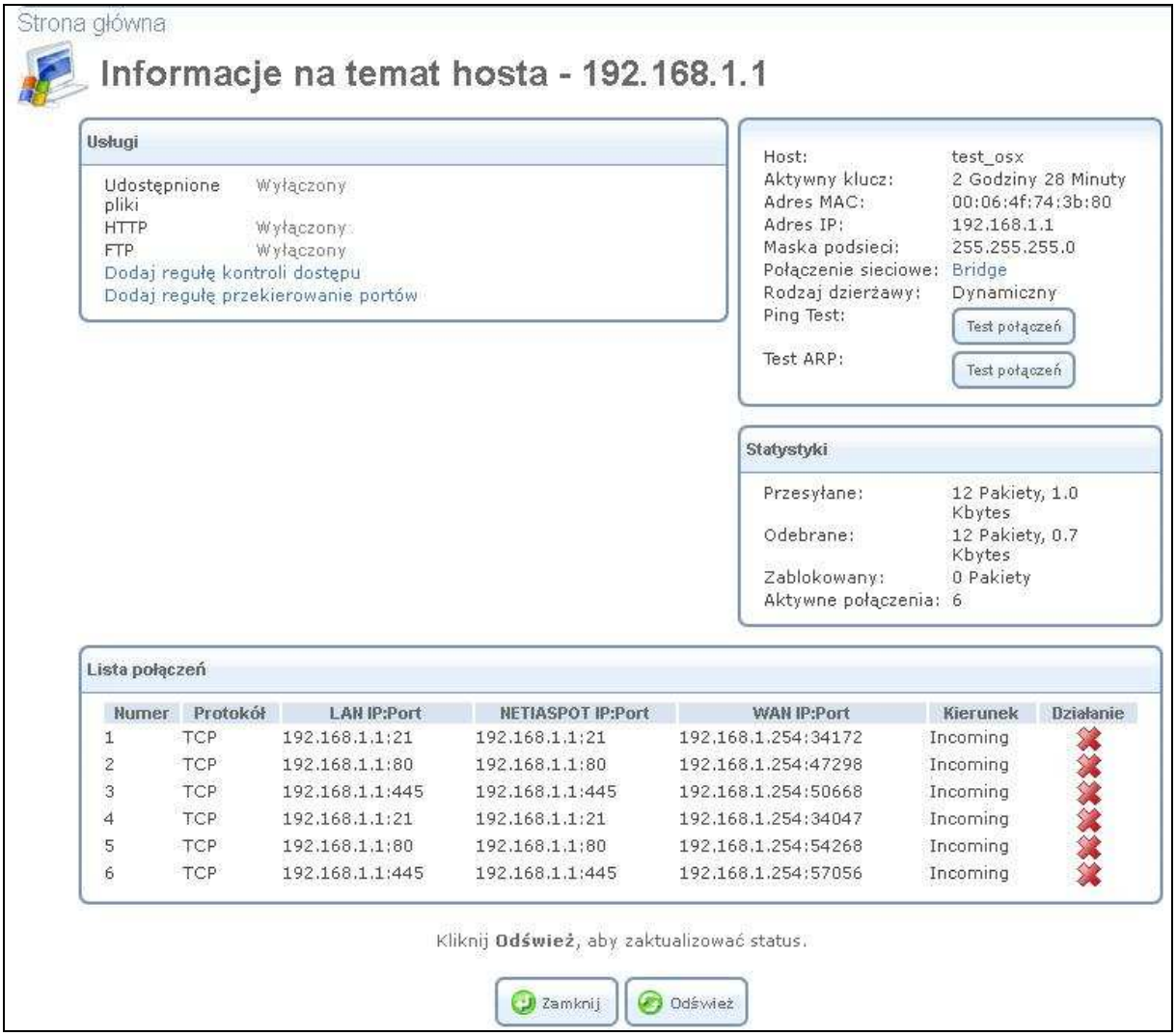


Rysunek 2.7 Połączony bezprzewodowo komputer

2.1.2. Przeglądanie sieci lokalnej

„Urządzenia sieciowe” w sekcji przeglądu podłączonych urządzeń w sieci lokalnej OpenRG, która obejmuje wszystkie komputery, co zostały podłączone do sieci naszego urządzenia. Adresy IP, prędkość połączenia (rysunek 2.1).

Aby wyświetlić więcej informacji na temat danego komputera, kliknij na link z odpowiednim odnośnikiem, aby zostały wyświetlone „Informacje na temat hosta”.



Rysunek 2.8 Informacje na temat hosta

Ekran ten przedstawia wszystkie istotne informacje o podłączonym komputerze, takie jak informacje o połączeniu, dostępnych usługach i statystykach ruchu.

Usługi – w tej sekcji wymieniono usługi na komputerze, które są dostępne na innych komputerach z sieci LAN. Gdy usługa jest dostępna z sieci LAN, można ją uaktywnić, klikając jej nazwę. Gdy usługa jest dostępna poprzez dostęp web, można ją włączyć, klikając przycisk „Dostęp do web".

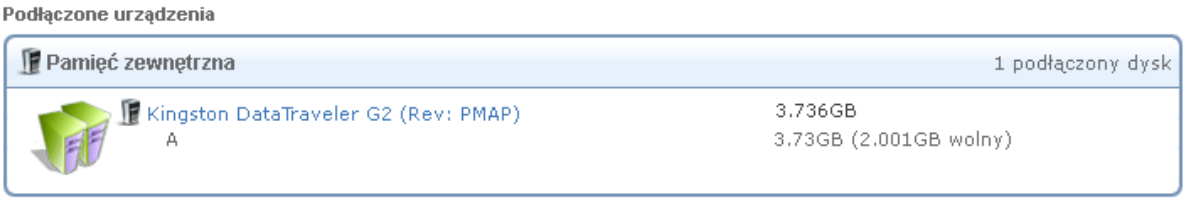
Informacje o połączeniu - ta sekcja wyświetla różne szczegóły dotyczące komputera, ustawienia połączeń.

Statystyki - sekcja wyświetla statystyki ruchu komputera, takie jak liczba i wielkość wysłanych i odebranych pakietów.

Lista połączeń - ta sekcja wyświetla listę połączeń otwartych przez komputer w zaporze sieciowej OpenRG. W tabeli wyświetlane są: źródłowy adresu IP w sieci LAN i port komputera, adres IP i port bramy, na który to adres i port jest tłumaczony i docelowy adres IP, port WAN.

2.1.3. Przegląd podłączonych urządzeń

Sekcja „Podłączonych urządzeń" wyświetla urządzenia peryferyjne podłączone do naszego urządzenia. Na przykład, podłącz urządzenie pamięci zewnętrznej i odśwież ekran.



Rysunek 2.9 podłączonego urządzenia magazynującego

2.1.4. Wyświetlenie stanu systemu

Sekcja „Status systemu" w zakładce „Strona główna" (patrz Rysunek 2.1) wyświetla następujące informacje:

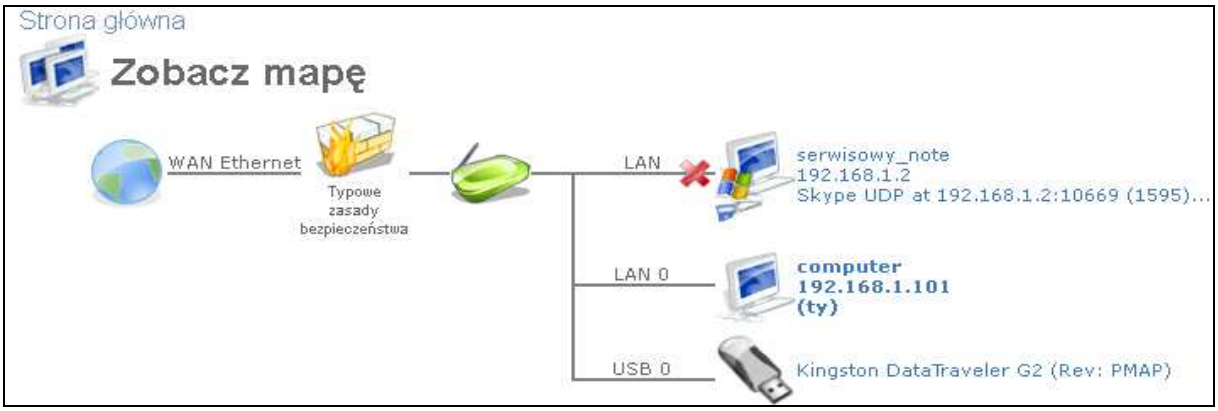
• Typ połączenia internetowego, dostępna prędkość i tryb transmisji danych. Kliknij na odnośnik „Połączenie internetowe", aby uzyskać więcej szczegółów.

• Wyświetla pierwszą piątkę aplikacji i komputerów zużywających przepustowość w odpowiednich sekcjach w kolejności malejącej. Aktualny downstream i upstream wolumenów zostaje wyświetlony dla każdej aplikacji i komputera.

• Informacje o systemie, zawiera ID urządzenia, wersje oprogramowania i czasu pracy urządzenia. Kliknij na nagłówek „Informacje o systemie", aby uzyskać więcej szczegółów.

2.2. Przeglądanie mapy sieci przy użyciu funkcji „Zobacz mapę”

Ekran „Zobacz mapę” wyświetla graficznie mapę sieci.



Rysunek 2.10 Strona główna – Zobacz mapę

Mapa sieci przedstawia różne elementy sieci, takie jak połączenia z internetem, zaporę sieciową, nasze urządzenie, lokalne komputery i urządzenia peryferyjne.

Ikona przedstawia Internet

Ikona przedstawia zaporę sieciową naszego urządzenia. Kliknij na tą ikonę, aby skonfigurować ustawienia zabezpieczeń. Więcej informacji można znaleźć w sekcji „Zapora sieciowa” instrukcji administracyjnej.

Ikona przedstawia nasze urządzenie

Mapa sieci dynamicznie reprezentuje obiekty sieciowe podłączone do naszego urządzenia. OpenRG rozpoznaje komercyjne systemy operacyjne i urządzeniach do gier, które są reprezentowane przez odpowiednie ikony.

Reprezentuje kablowe i bezprzewodowe komputery (hosty) połączona z naszym urządzeniem. Taki host jest też klientem DHCP, który otrzymał od OpenRG IP dzierżawy, lub może to być host ze statycznym adresem IP, automatycznie wykryty przez OpenRG. Należy pamiętać, że OpenRG rozpoznaje fizycznie połączony host i wyświetla go w mapie sieci tylko, gdy jego aktywność w sieci została wykryta (np. próba przejścia do panelu konfiguracyjnego, lub gdy host korzysta z internetu). Kliknij ikonę danego hosta w mapie sieci, aby wyświetlić szczegółowe informacje dla odpowiedniego hosta.

Reprezentuje komputery, których dzierżawy DHCP wygasły i nie były odnawiane. DHCP jest odnawiane automatycznie, chyba że host nie jest już fizycznie podłączony do OpenRG. Odłączony host zniknie z mapy sieci w czasie kolejnego zapytania dzierżawy IP, przez serwer DHCP OpenRG. **Uwaga:** Ta ikona oznacza także statyczne IP hosta, który nie jest aktywny w sieci..

Ikona przedstawia host Windows™ podłączony do naszego urządzenia.

Ikona przedstawia bezprzewodowy host podłączony do naszego urządzenia.

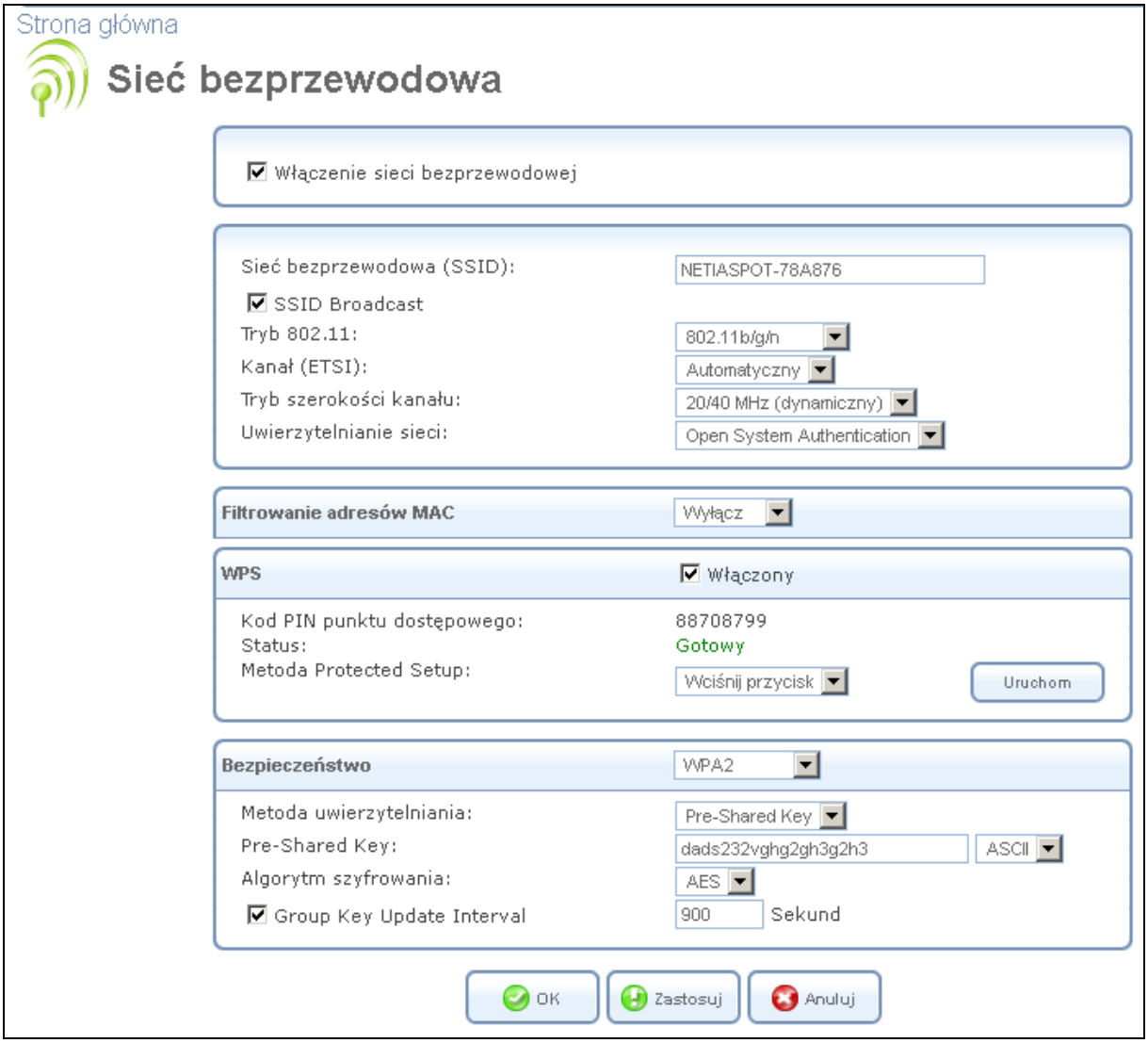
Ikona przedstawia USB podłączony do naszego urządzenia.

Ikona przedstawia dysk twardy USB podłączony do naszego urządzenia.

Standardowa mapa sieci OpenRG wyświetla urządzenia, które nasze urządzenie rozpoznało i przyznało dzierżawę DHCP.

2.3. Konfiguracja sieci bezprzewodowej

Pozycja „Sieć bezprzewodowa" pozwala na przeglądanie i konfigurowanie ustawień punktu dostępu bezprzewodowego wbudowanego w nasze urządzenie.



Rysunek 2.11 Ustawienia – Sieć bezprzewodowa

Włączenie sieci bezprzewodowej - zaznacz lub wyczyść pole wyboru, aby włączyć lub wyłączyć interfejs sieci bezprzewodowej.

Sieć bezprzewodowa (SSID) - SSID to nazwa sieci bezprzewodowej, współdzielona przez wszystkie punkty w sieci bezprzewodowej. Wielkość liter jest istotna, nazwa nie może przekraczać 32 znaków. Pamiętaj, że możesz używać tylko znaków ASCII. Aby zwiększyć bezpieczeństwo, można zmienić domyślne SSID na unikatową nazwę.

SSID Broadcast (rozgłaszanie) - domyślnie OpenRG transmituje nazwę sieci bezprzewodowej (SSID). Ze względów bezpieczeństwa, można ukryć w sieci bezprzewodowej rozgłaszanie nazwy sieci naszego urządzenia poprzez odznaczenie tej

opcji. Klienci łączący się do naszej sieci bezprzewodowej będą mogli łączyć się przez ręczne wpisanie SSID w aplikacji klienckich karty bezprzewodowej (Windows lub aplikacji innej firmy), a nie wybierając, jak wcześniej nazwę sieci bezprzewodowej z listy dostępnych sieci bezprzewodowych.

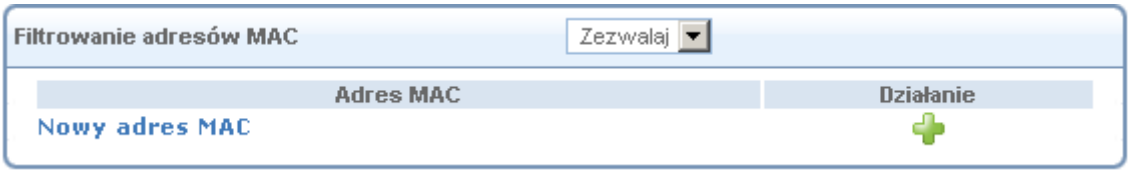
Tryb 802.11 - wybierz żądany typ połączenia bezprzewodowego. Domyślnie jest ustawiony na 802.11g/n. Należy pamiętać, że starsze urządzenia 802.11b nie są zgodne z trybem 802.11g/n oraz samym 802.11g.

Kanał - wszystkie urządzenia w sieci bezprzewodowej nadają na różnych kanałach. Pozostawianie tego parametru jako „Automatyczny" zapewnia sprawdzanie na bieżąco przez OpenRG dostępnych kanałów w sieci bezprzewodowej na danym obszarze. Możliwe jest też, aby wybrać kanał ręcznie, jeśli posiadamy informacje dotyczące kanałów bezprzewodowy używanych, w naszym otoczeniu.

Tryb szerokości kanału – wybierz szerokości kanału dla sieci bezprzewodowej, w zależności od wybranego standardu komunikacji. Dla „b" oraz „g", wybierz opcję „Tylko 20 MHz" lub „20/40 MHz (dynamiczny)". W trybie 802.11n mogą być wybrane dowolne ustawienia.

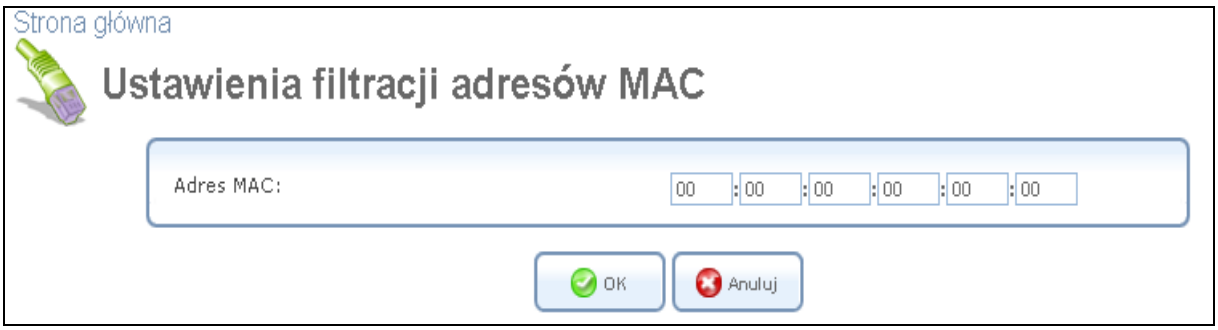
Uwierzytelnianie sieci - metoda uwierzytelnienia WPA „Open System Authentication" oznacza, że klucz sieciowy nie jest używany do uwierzytelniania. Używając protokołów zabezpieczeń 802.1X WEP lub Non-802.1X WEP, możemy zmienić i wybrać z rozwijanego menu metodę „Shared Key Authentication" (która korzysta ze współdzielonego klucza sieciowego do uwierzytelniania) lub możemy wybrać obie metody łącznie.

MAC Filtering – można filtrować klientów bezprzewodowych w zależności od ich adresu MAC, zezwalać lub odmawiając im dostępu do sieci bezprzewodowej. Aby dodać regułę filtrowania MAC, należy wybrać akcję do wykonania w rozwijanym menu. Następnie kliknij przycisk „Nowy adres MAC". Ekran ustawień filtracji adresów MAC jest widoczny poniżej.



Rysunek 2.12 Filtrowanie adresów MAC

Wpisz adres MAC, który ma być filtrowany i kliknij „OK.”. Wprowadzony adres MAC pojawi się w tabeli.



Rysunek 2.13 Dodawanie wpisu do filtracji adresów MAC

Zauważ, że gdy zaznaczona jest opcja „Zezwalaj”, tylko klienci bezprzewodowi, których adresy MAC są dopisane, w tej tabeli będą mogli się połączyć. Gdy wybrana jest opcja „Odrzuć”, wszystkie wymienione wpisy adresów MAC klientów bezprzewodowych nie będą mogli się połączyć.

Wi-Fi Protected Setup (WPS) - WPS to metoda uproszczenia konfiguracji zabezpieczeń i zarządzania sieciami bezprzewodowymi.

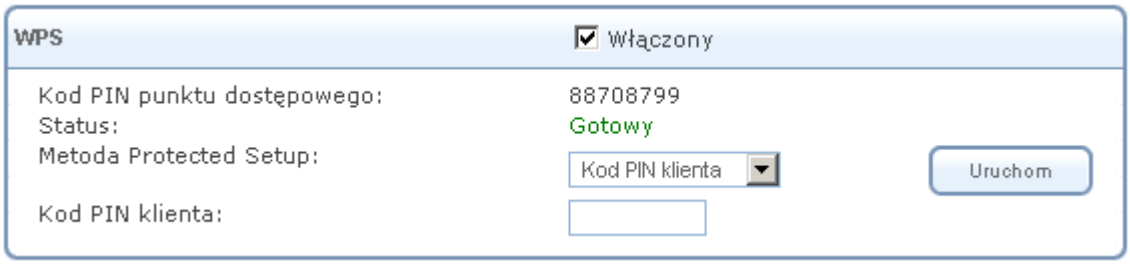
Status określa stan WPS. Status oznaczony jako „Gotowy” oznacza, że system jest gotowy do negocjacji przychodzących od klientów bezprzewodowych, lub „rejestrujących”.

Metoda Protected Setup - OpenRG obsługuje dwie metody połączenia „Push Button” (metoda domyślna) i „PIN kod klienta”. Są to metody stosowane przez klientów bezprzewodowych w poszukiwaniu punktu dostępu wspierającego WPS.

• **Push Button** (naciśnij przycisk) - rejestracja jest inicjowana przez fizyczne wciśnięcie przycisku na karcie bezprzewodowej klienta lub poprzez oprogramowanie. Po rozpoczęciu

rejestracji, kliknij przycisk „Uruchom” lub naciśnij przycisk WPS znajdujący się na tyle urządzenia, aby twoje urządzenie oczekiwało na połączenie ze stacji klienckiej.

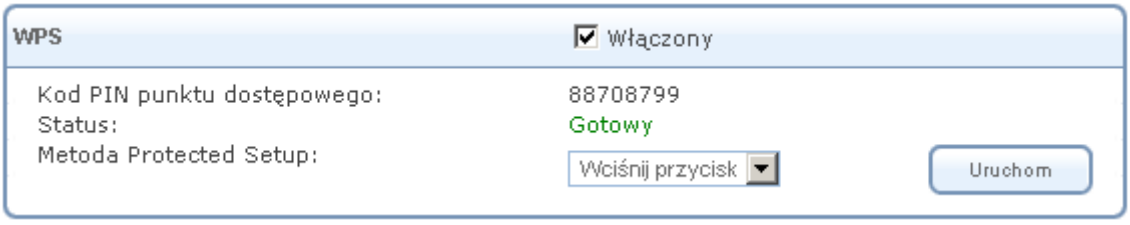
• **Kod PIN klienta** - rejestracja jest inicjowana przez oprogramowanie klienta bezprzewodowego, które musi wspierać metodę kodu PIN. Aby uzyskać połączenie w ten sposób, należy wybrać tę opcję z menu rozwijanego. Zostanie wyświetlone pole do wprowadzenia kodu PIN.



Rysunek 2.14 Metoda automatycznej konfiguracji zabezpieczeń – Kod PIN

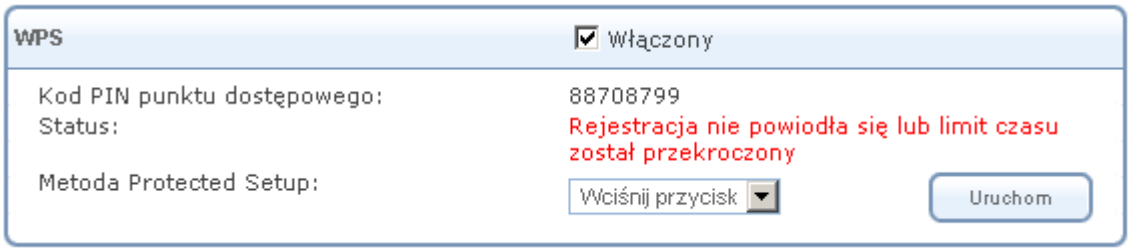
W tym polu wprowadź czterocyfrowy kod PIN dostarczony przez oprogramowanie klienta bezprzewodowego. Kliknij przycisk „Uruchom” w urządzeniu, aby nawiązać połączenie.

Przed podłączeniem klienta sieci bezprzewodowej do sieci bezprzewodowej OpenRG przy wykorzystaniu WPS, musimy wiedzieć, z jakiej metody automatycznej konfiguracji będziemy korzystać. Po wciśnięciu przycisku WPS nasze urządzenie będzie czekać dwie minuty na klienta chcącego uzyskać połączenie. Gdy połączenie zostanie ustanowione, pole „Status” zmieni status, aby o tym poinformować.



Rysunek 2.15 Status funkcji WPS

Należy pamiętać, że funkcja WPS jest obsługiwana tylko z zabezpieczeniem WPA. Dlatego też, gdy korzystamy z „WEP" lub sieci niezabezpieczonej, wybranych z rozwijanego menu „Zabezpieczenia", pojawi się poniższy komunikat w sekcji WPS.



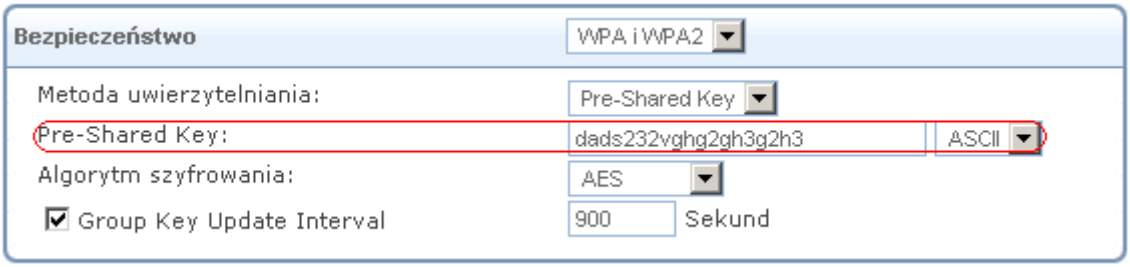
Rysunek 2.16 Połączenie WPS nie zostało nawiązane

Bezpieczeństwo sieci bezprzewodowej

Sekcja zabezpieczenia transmisji bezprzewodowej. Aby skonfigurować ustawienia zabezpieczeń sieci bezprzewodowej wybierz rodzaj i odpowiedni protokół zabezpieczeń z rozwijanego menu. Po odświeżeniu ekranu, przedstawia on odpowiednie protokoły konfiguracji.

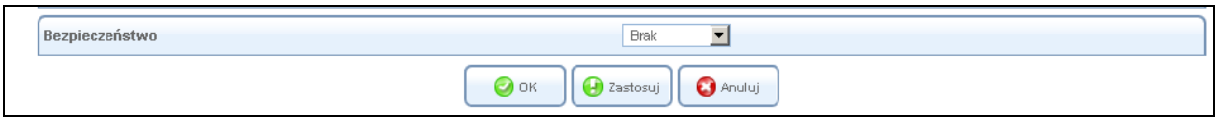
• WPA i WPA2 - mieszana metoda szyfrowania danych, która wykorzystuje WPA i WPA2.

Hasło sieci bezprzewodowej – to hasło wymagane do połączenia z naszym urządzeniem w sieci bezprzewodowej. Możesz zmienić domyślne hasło przez kliknięcie w sekcji „Bezpieczeństwo" i wprowadzenie hasła w polu „Pre-Shared Key", następnie klikając przycisk „Zastosuj". Hasło musi mieć co najmniej 8 znaków. Zauważ, że klikając przycisk „Reset" urządzenie przywróci domyślne hasło.



Rysunek 2.17 WPA i WPA2

• **Niezabezpieczona** - wybranie tej opcji wyłącza zabezpieczenia połączenia bezprzewodowego. Każdy bezprzewodowy komputer w danym obszarze będzie w stanie połączyć się z Internetem przy użyciu naszego połączenia **(opcja niezalecana).**

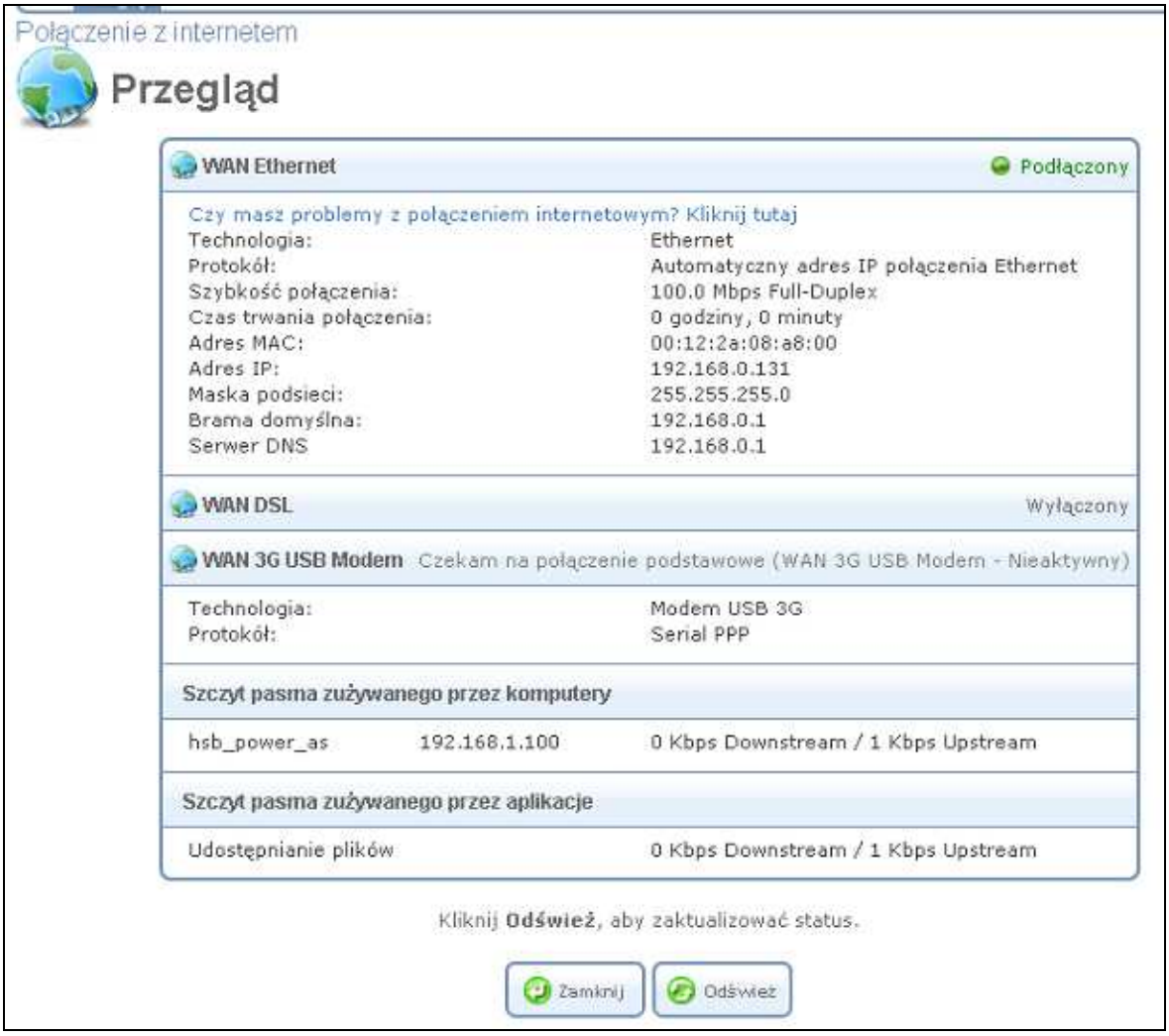


Rysunek 2.20 Wyłączone zabezpieczenia sieci bezprzewodowej

3. Połączenie z internetem

3.1. Przeglądanie właściwości twojego połączenia z Internetem

Ekran „Przegląd" zawiera ogólne informacje dotyczące połączenia z Internetem, takie jak status połączenia, protokół, szybkość, czas trwania, a także dane na temat zewnętrznego adresu IP i parametrów sieci. Możesz użyć tego ekranu, aby szybko wyświetlić swój status połączenia z Internetem.



Rysunek 3.1 Przegląd połączenia z Internetem

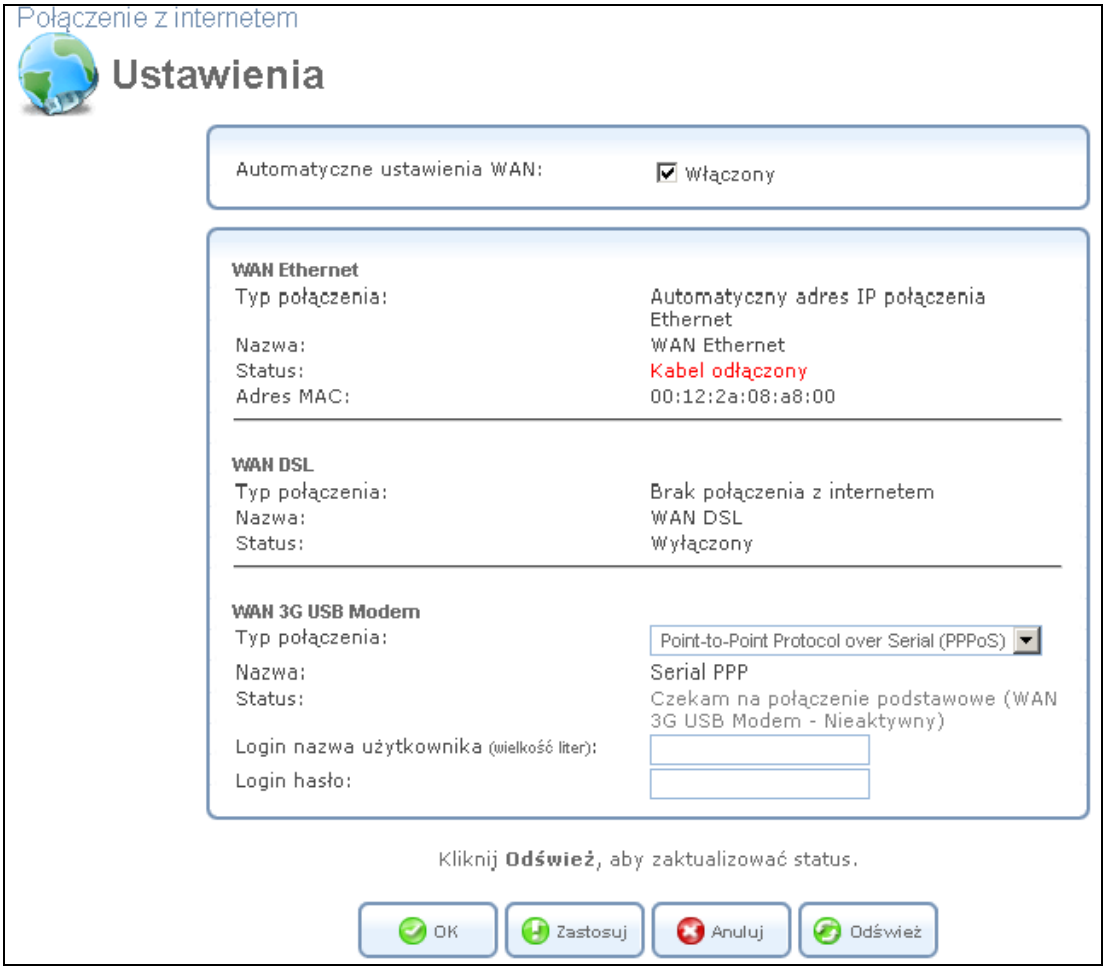
W menu „Przegląd" poniższe odnośniki pomocy są dostępne:

• **Masz problem z połączeniem internetowym? Kliknij tutaj** - link to ekran pomocy „Rozwiązywanie problemów", gdzie można uruchomić testy w celu zdiagnozowania i rozwiązywania problemów łączności z Internetem.

• **Kliknij tutaj, aby sprawdzić wykorzystanie połączenia internetowego.** Kliknij na ten link, aby wykonać analizę wykorzystania ruchu połączeń WAN. Dodatkowo, ekran wyświetla zapotrzebowanie na nasze pasmo aplikacji i komputerów.

3.2 Konfiguracja połączenia z Internetem

Ekran „Ustawienia" zawiera podstawowe opcje konfiguracji dla różnych typów połączeń internetowych obsługiwanych przez OpenRG. Funkcja „Automatyczne ustawienia WAN" jest domyślnie włączona, co oznacza, że nasze urządzenie będzie automatycznie rozpoznawać rodzaj połączenia fizycznego, które jest podłączone, Ethernet lub DSL.

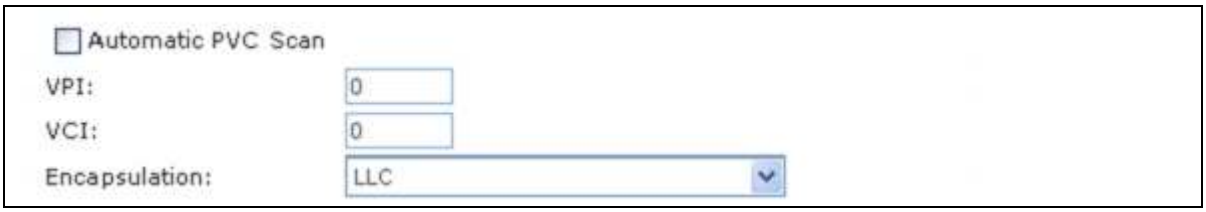


Rysunek 3.2 Połączenie z Internetem – Ustawienia

Jeśli jesteś już podłączony do Internetu, to ekran będzie wyświetlał informacje o dostępnych połączeniach. Na przykład, gdy wybrany typ połączenia, to np. PPPoE możemy skonfigurować następujące parametry:

- **Nazwa użytkownika (login) i hasło** – są to dane logowania dostarczane przez ISP.
- **Automatyczne skanowanie PVC** - to pole wyboru jest domyślnie włączone, co oznacza, że OpenRG automatycznie konfiguruje parametry enkapsulacji VPI i VCI.

Jeśli chcieliby Państwo skonfigurować te parametry, proszę usunąć zaznaczenie obok tego pola wyboru. Po odświeżeniu ekranu, możemy te wartości wpisać ręcznie.

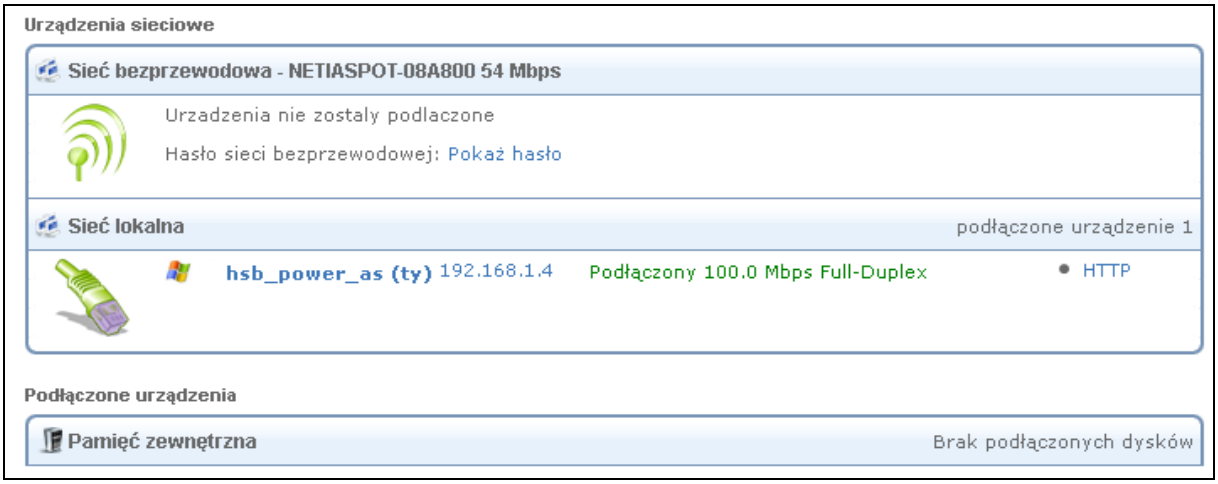


Rysunek 3.3 Ręczne określenie parametrów PVC

Uwaga: Błąd w konfiguracji tych parametrów może uniemożliwić poprawną pracę naszego połączenia ADSL. Dlatego zalecane jest upewnienie się, jakie parametry powinniśmy wpisać. Parametry VPI/VCI dla łącza Netii to 8/35, a jeśli posiadamy łącze Netii na liniach innego operatora np. TPSA wtedy będzie to: 0/35

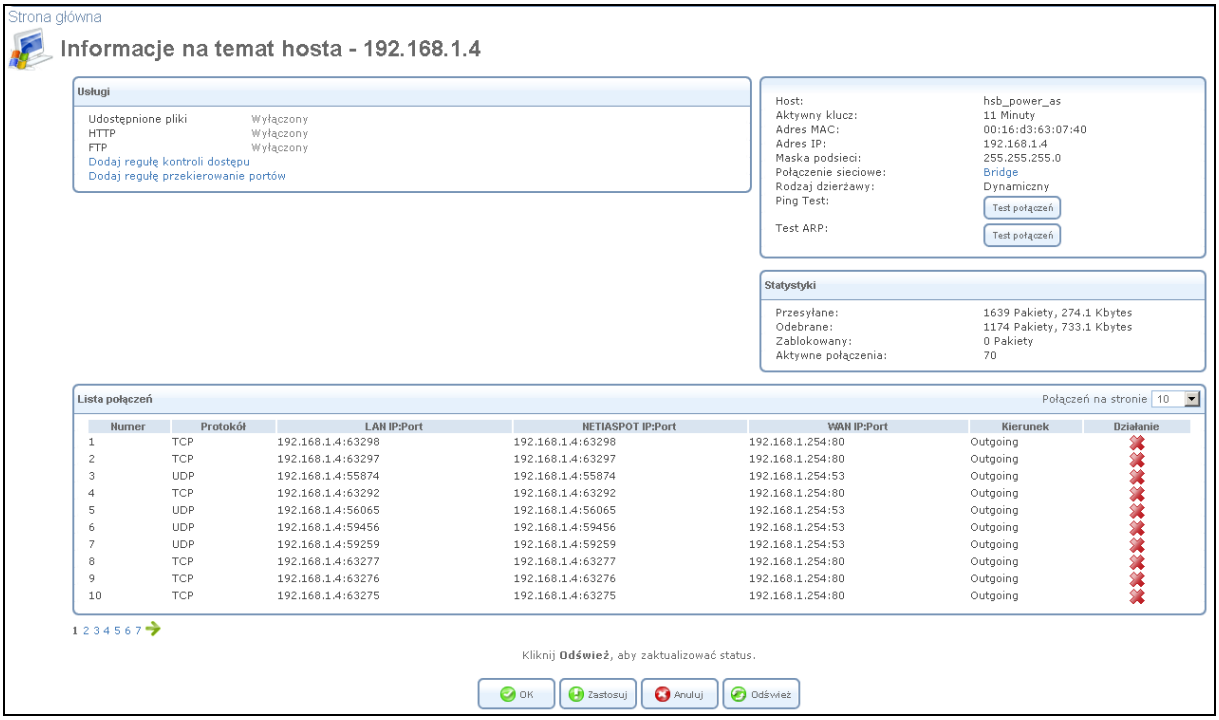
4. Sieć lokalna

4.1. Przegląd naszej sieci lokalnej



Rysunek 4.1 Przegląd sieci lokalnej

Aby wyświetlić więcej informacji na temat danego komputera, kliknij jego odpowiednik (odnośnik). Wyświetlony zostanie ekran z informacjami na temat danego hosta.



Rysunek 4.2 Informacje na temat hosta

Ekran ten przedstawia wszystkie informacje istotne o podłączonym komputerze, takie jak ustawienia połączeń, dostępne usługi, statystyki ruchu i listę połączeń. Umożliwia także wykonywanie testów połączeń z komputerem.

Sekcja ta zawiera usługi włączone na komputerze, które są dostępne dla innych komputerów w sieci LAN. Gdy usługa jest dostępna z sieci LAN, można ją uaktywnić poprzez kliknięcie na jej nazwę lub wyświetlony adres URL (patrz rysunek 4.2). Gdy usługa jest dostępna za pośrednictwem dostępu przez stronę internetową, można ją włączyć, klikając odnośnik „Dostęp web", który pojawi się jeśli usługa będzie dostępna. Dostępne usługi to:

• **Udostępnione pliki** - dostęp do udostępnionych plików komputera.
• **HTTP** - dostęp do serwera HTTP komputera (jeśli jest dostępny).
• **FTP** – otwarcie sesji FTP z komputerem.
• **Telnet** – otwarcie sesji Telnet z komputerem.
• **Zdalny pulpit** - Zdalne sterowanie komputerem z systemem Windows za pomocą narzędzia „Pulpit zdalny".

• **VNC** - zdalne sterowanie komputerem za pomocą protokołu „Virtual Network Computing”.

• **Dodaj regułę kontroli dostępu** - blokowanie dostępu do usług internetowych z komputera, lub umożliwienie takiego dostępu, jeśli zapora jest ustawiona w trybie wysokiego poziomu bezpieczeństwa (więcej informacji znajduje się w rozdziale 5.2.2).

• **Dodaj regułę przekierowania portu** - usługa wystawienia na komputerze usługi, dla zewnętrznych użytkowników Internetu (więcej informacji można znaleźć w sekcji 5.2.3).

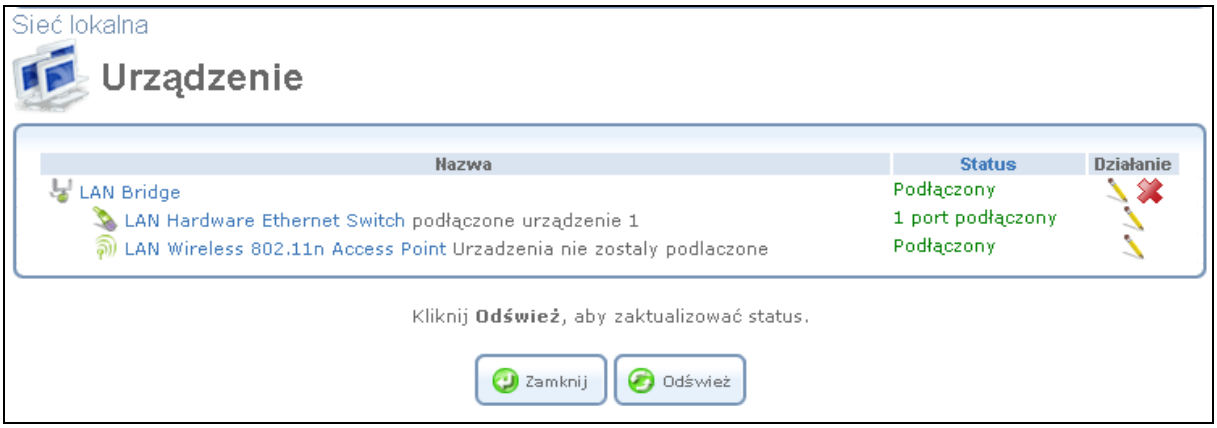
Informacje o połączeniu - sekcja wyświetla różne szczegóły dotyczące połączeń komputera. Ponadto, można uruchomić test połączenia „Ping” lub „ARP”, klikając na przycisk odpowiedni przycisk „Test połączenia”. Badania wykonywane są w ekranie „Diagnostyka” (patrz punkt 6.8.3).

Statystyki - sekcja wyświetla statystyki ruchu komputera, takie jak liczba i wielkość wysyłanych i odbieranych pakietów.

Lista połączeń - sekcja wyświetla listę połączeń otwartych przez komputer na zaporze sieciowej OpenRG. W tabeli wyświetlane są źródłowego adres IP/port komputera w sieci LAN, adres IP i port bramy, do której pakiet jest przekazywany i docelowy adres IP/port WAN.

4.2. Przegląd urządzeń w naszej sieci LAN

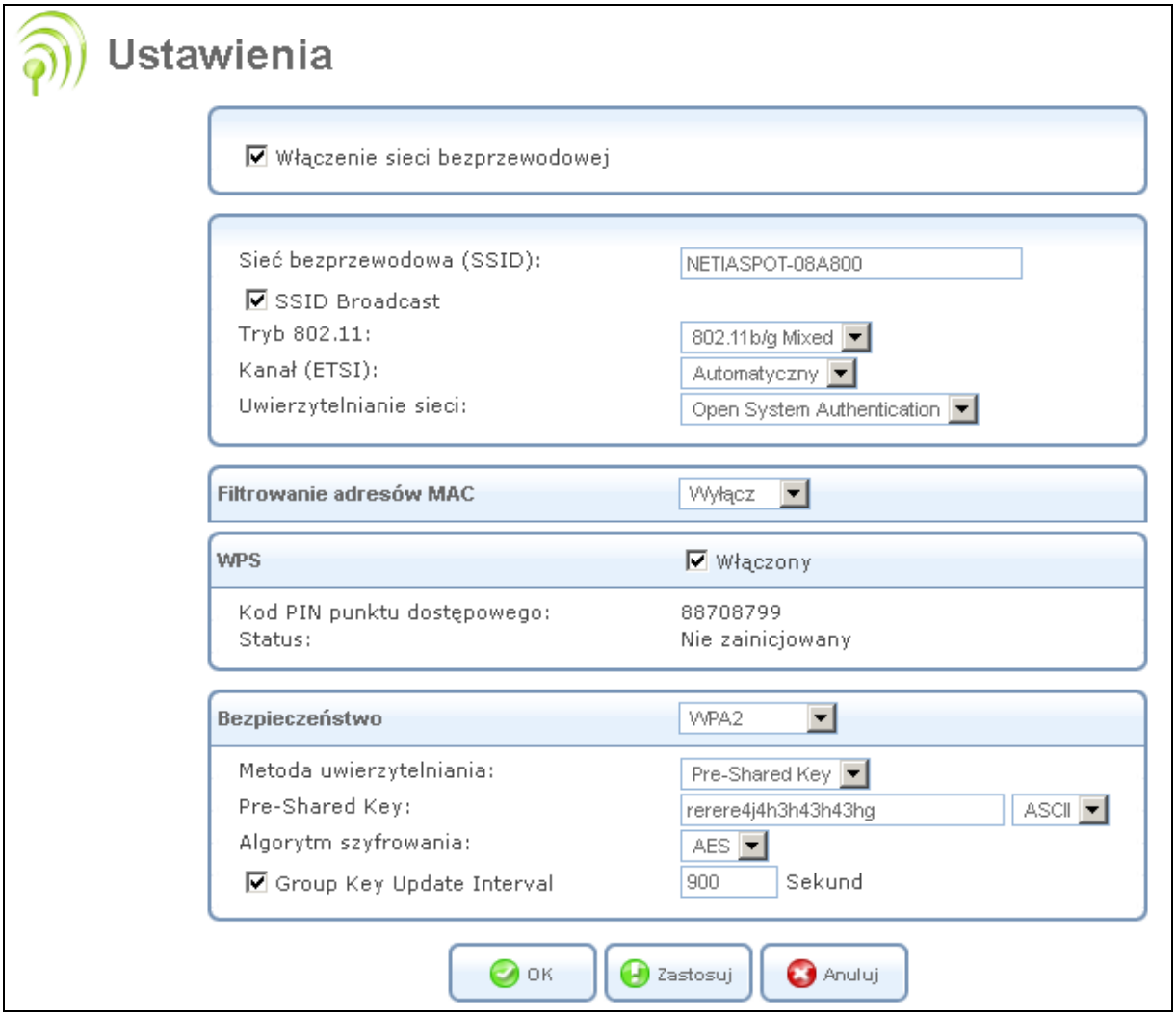
Sekcja „Urządzenie” (patrz Rysunek 4.3) przedstawia zestawienie urządzeń sieci LAN OpenRG, w tym mosty sieciowe (bridge), Ethernet (LAN), USB, sieć bezprzewodową i stan każdego z nich (podłączony/odłączony).



Rysunek 4.3 Przegląd urządzeń w sieci lokalnej

4.3. Konfiguracja naszej sieci bezprzewodowej

Sekcja „Sieć bezprzewodowa" koncentruje się na ustawieniach sieci bezprzewodowej LAN. Ekran ten przedstawia ustawienia sieci bezprzewodowej OpenRG i pozwala je zmienić w zależności od potrzeb.



Rysunek 4.4 Przegląd ustawień sieci bezprzewodowej

Uwaga: Błąd w konfiguracji interfejsu bezprzewodowego może uniemożliwić jego poprawną pracę i problemy z połączeniem bezprzewodowym. Dlatego zalecane jest powstrzymanie się od zmian w ustawieniach domyślnych, chyba że posiadasz dostateczną wiedzę na temat modyfikowanych funkcji.

Włączenie sieci bezprzewodowej - zaznacz lub wyczyść to pole wyboru, aby włączyć lub wyłączyć interfejs sieci bezprzewodowej.

Sieć bezprzewodowa (SSID) - SSID to nazwa sieci, współdzielona przez wszystkie punkty w naszej sieci bezprzewodowej. Istotna jest wielkość wpisanych liter, nazwa nie może przekraczać 32 znaków. Pamiętaj, że możesz używać tylko znaków ASCII. Aby zwiększyć bezpieczeństwo, można zmienić domyślną unikatową nazwę SSID na inną.

SSID Broadcast - domyślnie OpenRG rozgłasza nazwę swojej sieci bezprzewodowej (SSID). Ze względów bezpieczeństwa, można ukryć rozgłaszanie nazwy sieci bezprzewodowej poprzez odznaczenie pola wyboru. Klienci sieci bezprzewodowej będą mogli łączyć się przez ręczne wpisanie SSID sieci bezprzewodowej w aplikacjach klienckich (Windows lub aplikacji innej firmy), po odznaczeniu rozgłaszania nie będzie możliwe wybranie jej z listy dostępnych sieci bezprzewodowych.

Tryb 802.11 - wybierz żądany typ połączenia bezprzewodowego. Domyślnie jest on ustawiony na 802.11g/n. Należy pamiętać, że starsze urządzenia 802.11b nie są zgodne z trybem 802.11g/n oraz samym 802.11g.

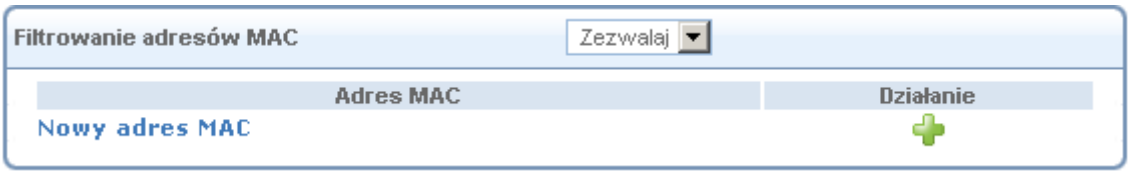
Kanał - wszystkie urządzenia w sieci bezprzewodowej używają do transmisji różnych kanałów. Wybranie tego parametru jako „Automatyczny" zapewnia OpenRG na bieżąco sprawdzenie możliwie najlepszego dostępnego kanału dla transmisji bezprzewodowej na danym obszarze. Możliwe jest, aby wybrać kanał ręcznie, jeśli sami posiadamy informacje dotyczące kanałów bezprzewodowych używanych w pobliżu naszego urządzenia.

Tryb szerokości kanału - szerokość kanału transmisji w sieci bezprzewodowej, jest zależna od wybranego standardu komunikacji w naszej sieci bezprzewodowej. Dla trybu „b" oraz „g", wybierz opcję „Tylko 20 MHz" lub „20/40 MHz (dynamiczny)". W trybie 802.11n może być wybrana każda z opcji.

Uwierzytelnianie sieci - metoda uwierzytelnienia WPA „Open System Authentication" oznacza, że klucz sieciowy nie jest używany do uwierzytelniania. Używając protokołów

zabezpieczeń 802.1X WEP lub Non-802.1X WEP możemy zmienić i wybrać z rozwijanego menu metodę „Shared Key Authentication" (która korzysta ze współdzielonego klucza sieciowego do uwierzytelniania) lub możemy wybrać obie metody łącznie.

MAC Filtering – można filtrować klientów bezprzewodowych w zależności od ich adresu MAC, zezwalać lub odmawiając im dostępu do sieci bezprzewodowej. Aby dodać regułę filtrowania MAC, należy wybrać akcję do wykonania w rozwijanym menu. Następnie kliknij przycisk „Nowy adres MAC". Ekran ustawień filtracji adresów MAC jest widoczny poniżej.



Rysunek 4.5 Filtrowanie adresów MAC

Wpisz adres MAC, który ma być filtrowany i kliknij „OK". Wprowadzony adres MAC pojawi się w tabeli.

Rysunek 4.6 Dodawanie wpisu do filtracji adresów MAC

Zauważ, że gdy zaznaczona jest opcja „Zezwalaj", tylko klienci bezprzewodowi, których adresy MAC są dopisane, w tej tabeli będą mogli się połączyć. Gdy wybrana jest opcja „Odrzuć", wszystkie wymienione wpisy adresów MAC klientów bezprzewodowych nie będą mogli się połączyć.

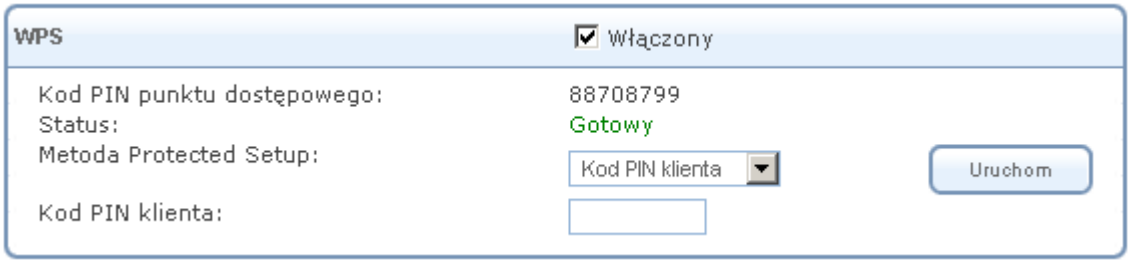
Wi-Fi Protected Setup (WPS) - WPS to metoda uproszczenia konfiguracji zabezpieczeń i zarządzania sieciami bezprzewodowymi.

Status określa stan WPS. Status oznaczony jako „Gotowy" oznacza, że system jest gotowy do negocjacji przychodzących od klientów bezprzewodowych, lub „rejestrujących".

Metoda Protected Setup - OpenRG obsługuje dwie metody połączenia „Push Button" (metoda domyślna) i „PIN kod klienta". Są to metody stosowane przez klientów bezprzewodowych w poszukiwaniu punktu dostępu wspierającego WPS.

• **Push Buton** (naciśnij przycisk) - rejestracja jest inicjowana przez fizyczne wciśnięcie przycisku na karcie bezprzewodowej klienta lub poprzez oprogramowanie. Po rozpoczęciu rejestracji, kliknij przycisk „Uruchom" lub naciśnij przycisk WPS znajdujący się na tyle urządzenia, aby Twoje urządzenie oczekiwało na połączenie ze stacji klienckiej.

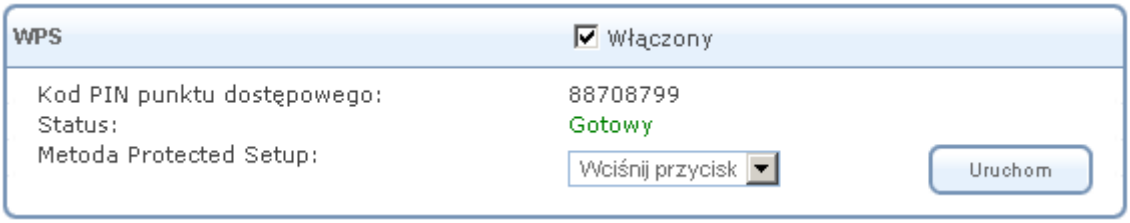
• **Kod PIN klienta** - rejestracja jest inicjowana przez oprogramowanie klienta bezprzewodowego, które musi wspierać metodę kodu PIN. Aby uzyskać połączenie w ten sposób, należy wybrać tę opcję z menu rozwijanego. Zostanie wyświetlone pole do wprowadzenia kodu PIN.



Rysunek 4.7 Metoda automatycznej konfiguracji zabezpieczeń – Kod PIN

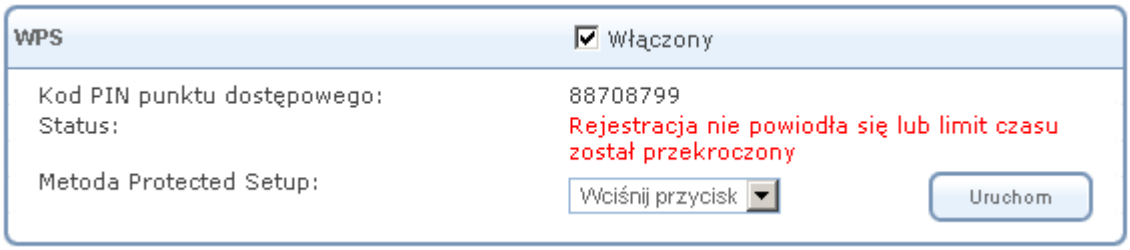
W tym polu wprowadź czterocyfrowy kod PIN dostarczony przez oprogramowanie klienta bezprzewodowego. Kliknij przycisk „Uruchom" w urządzeniu, aby nawiązać połączenie.

Przed podłączeniem klienta sieci bezprzewodowej do sieci bezprzewodowej OpenRG przy wykorzystaniu WPS, musimy wiedzieć, z jakiej metody automatycznej konfiguracji będziemy korzystać. Po wciśnięciu przycisku WPS nasze urządzenie będzie czekać dwie minuty na klienta chcącego uzyskać połączenie. Gdy połączenie zostanie ustanowione, pole „Status" zmieni status, aby o tym poinformować.



Rysunek 4.8 Status funkcji WPS

Należy pamiętać, że funkcja WPS jest obsługiwana tylko z zabezpieczeniem WPA. Dlatego też, gdy korzystamy z „WEP" lub sieci niezabezpieczonej, wybranych z rozwijanego menu „Zabezpieczenia", pojawi się poniższy komunikat w sekcji WPS.



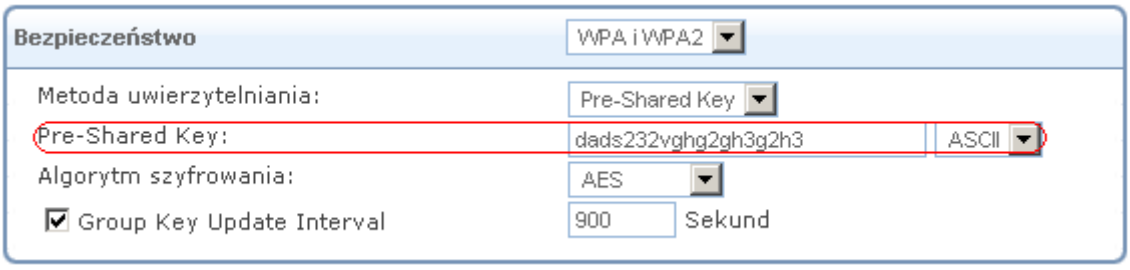
Rysunek 4.9 Połączenie WPS nie zostało nawiązane

Bezpieczeństwo sieci bezprzewodowej

Sekcja zabezpieczenia transmisji bezprzewodowej, aby skonfigurować ustawienia zabezpieczeń sieci bezprzewodowej wybierz rodzaj odpowiedni protokół zabezpieczeń z rozwijanego menu. Po odświeżeniu ekranu, przedstawia on odpowiednie protokoły konfiguracji.

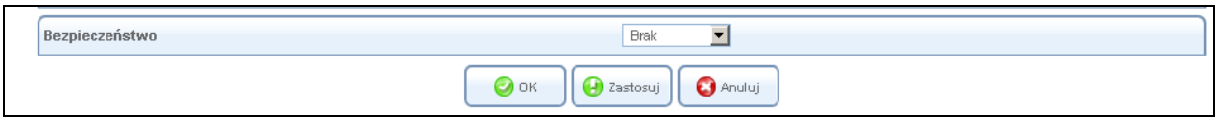
• WPA i WPA2 - mieszana metoda szyfrowania danych, która wykorzystuje WPA i WPA2.

Hasło sieci bezprzewodowej – to hasło wymagane do połączenia z naszym urządzeniem w sieci bezprzewodowej. Możesz zmienić domyślne hasło przez kliknięcie w sekcji „Bezpieczeństwo" i wprowadzeniu hasła w polu „Pre-Shared Key", następnie klikając przycisk „Zastosuj". Hasło musi mieć co najmniej 8 znaków. Zauważ, że klikając przycisk „Reset" urządzenie przywróci domyślne hasło.



Rysunek 4.10 WPA i WPA2

• **Niezabezpieczona** - wybranie tej opcji wyłącza zabezpieczenia połączenia bezprzewodowego. Każdy bezprzewodowy komputer w danym obszarze będzie w stanie połączyć się z Internetem przy użyciu naszego połączenia **(opcja niezalecana).**



Rysunek 4.13 Wyłączone zabezpieczenia sieci bezprzewodowej

5. Usługi

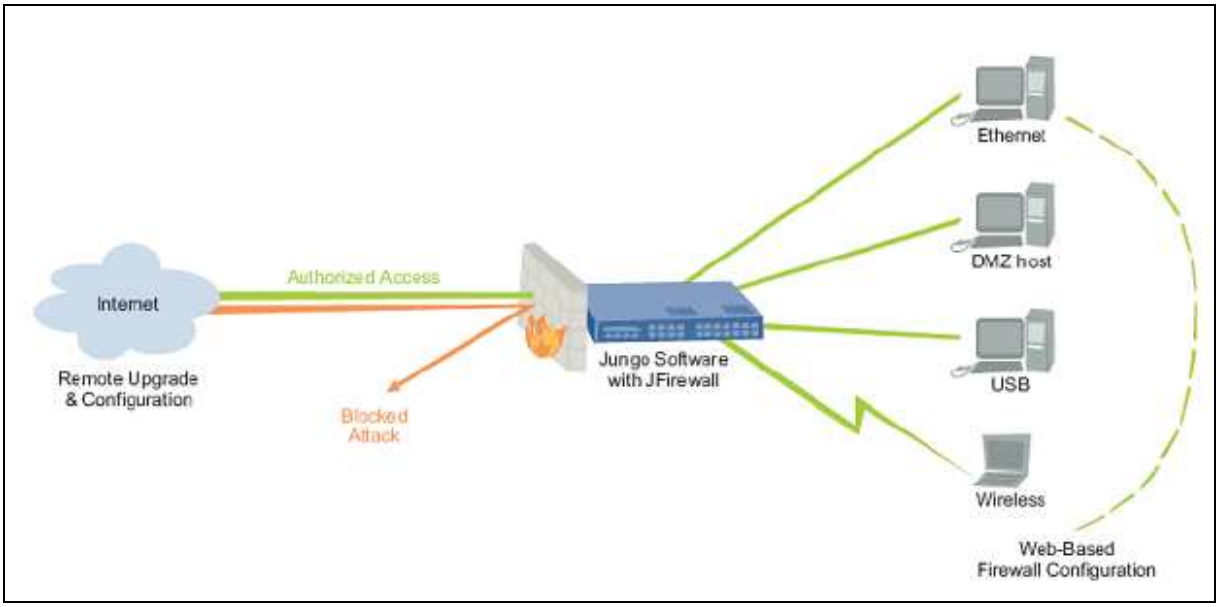
5.1 Przegląd dostępnych usług

Ekran „Przegląd" prezentuje podsumowanie usług OpenRG i ich aktualny status (włączona/wyłączona). Usługi te są konfigurowalne poprzez ich pozycje w menu zakładki „Usługi".

Rysunek 5.1 Przegląd dostępnych usług

5.2 Zabezpieczenie sieci z użyciem zapory sieciowej OpenRG

Rozdział bezpieczeństwa urządzenia OpenRG obejmuje kompleksowe i solidne zabezpieczenia usług „Stateful Packet Inspection Firewall", protokoły uwierzytelniania użytkownika oraz mechanizmy ochrony hasłem. Te funkcje pozwalają użytkownikom podłączyć swoje komputery do Internetu, a jednocześnie chronić podłączone komputery przed zagrożeniami z Internetu. Zapora sieciowa, RG-FW OpenRG ™ odpowiada za bezpieczeństwo urządzenia i podłączonych klientów, została specjalnie dostosowana do potrzeb domowych i biurowych użytkowników. Została skonfigurowana w celu zapewnienia optymalnego bezpieczeństwa (patrz rysunek 5.2).



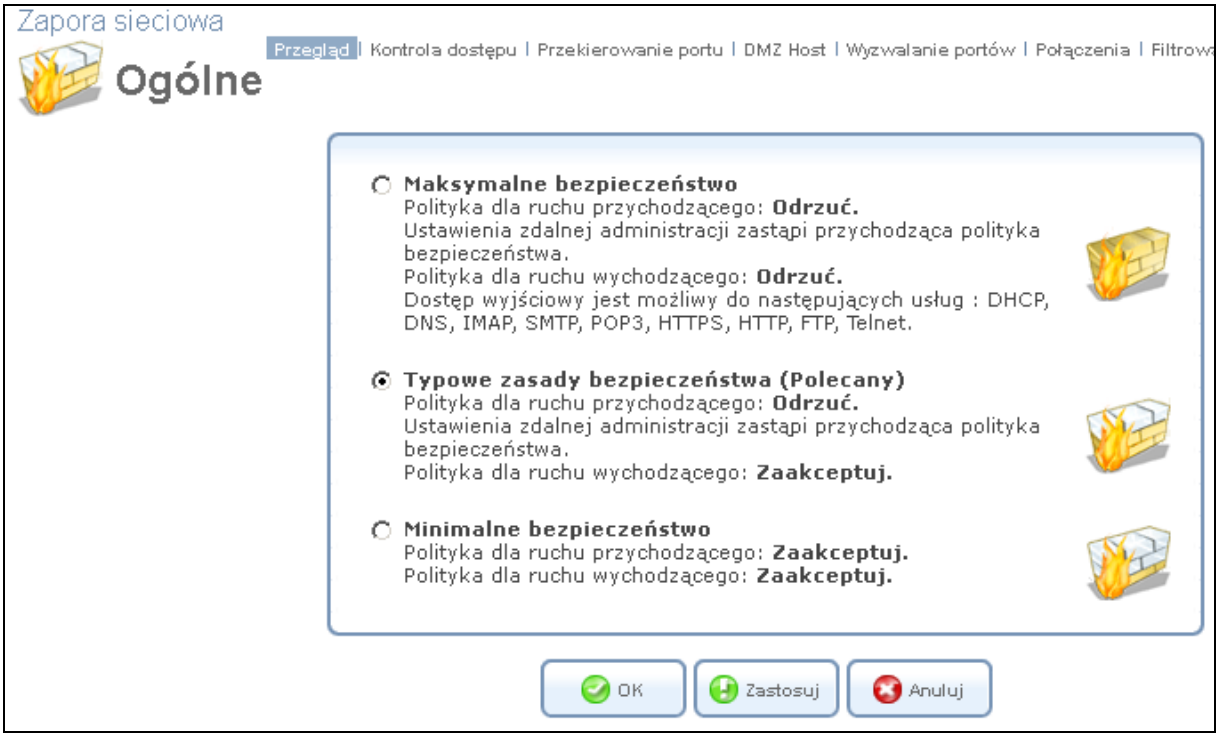
Rysunek 5.2 Zapora sieciowa OpenRG w akcji

Zapora sieciowa OpenRG zapewnia zarówno bezpieczeństwo, jak i elastyczność użytkowników domowych i biurowych. Zapewnia profesjonalny poziom bezpieczeństwa sieci i umożliwia bezpieczne korzystanie z interaktywnych aplikacji, takich jak gry internetowe i wideo-konferencji.

Dodatkowe funkcje, w tym ograniczenia przeglądania i kontroli dostępu, może być łatwo konfigurowane lokalnie przez użytkownika poprzez przyjazny interfejs użytkownika z poziomu przeglądarki internetowej, albo zdalnie przez dostawcę usług. Zapora sieciowa OpenRG obsługuje zaawansowane filtrowanie, jest zaprojektowana w sposób umożliwiający pełną kontrolę nad zaporą sieciową. Możesz określić szczegółowe zasady wejścia i wyjścia, kontrole kolejności logicznie podobnych zbiorów, przepisów i wprowadzać rozróżnienia zasad, które obowiązują urządzenia sieciowe WAN i LAN.

5.2.1. Konfiguracja podstawowych ustawień zabezpieczeń

Ekran przedstawia „Przegląd" zapory, można skonfigurować podstawowe ustawienia bezpieczeństwa naszego urządzenia.



Rysunek 5.3 Zapora sieciowa – Przegląd

Możesz wybrać jeden z trzech predefiniowanych poziomów ochrony zapory sieciowej OpenRG: „Minimalne bezpieczeństwo", „Typowe zasady bezpieczeństwa" (domyślny) i „Maksymalne bezpieczeństwo". Poniższa tabela podsumowuje zachowanie OpenRG przy każdym z trzech poziomów ochrony.

Poziom bezpieczeństwa	**Żądania pochodzące z sieci WAN (ruch przychodzący)**	**Żądania pochodzące z sieci WAN (ruch wychodzący)**
Maksymalne bezpieczeństwo	*Zablokowane:* Brak dostępu do strony głównej z sieci internetowej, z wyjątkiem skonfigurowanej w sekcjach przekierowania portów, DMZ i zdalnego dostępu.	*Ograniczenia:* Tylko wspólnie używane usługi są dozwolone, takie jak przeglądanie www i e-mail. Listy dozwolonych usługi mogą być edytowane w sekcji kontroli dostępu (patrz w punkcie 5.2.2)

Typowe bezpieczeństwo (Domyślne)	*Zablokowane:* Brak dostępu do strony głównej z sieci internetowej, z wyjątkiem konfiguracji w sekcji przekierowania portów, DMZ i zdalnego dostępu	*Nieograniczone:* Wszystkie usługi są dozwolone, z wyjątkiem skonfigurowanych w sekcji kontroli dostępu
Minimalne bezpieczeństwo	*Nieograniczone:* Pozwala na całkowity dostęp z Internetu do sieci domowej, wszystkie połączenia są dozwolone	*Nieograniczone:* Wszystkie usługi są dozwolone, z wyjątkiem skonfigurowanych w sekcji kontroli dostępu

Tabela 5.1 Poziomy zabezpieczeń zapory sieciowej OpenRG

Aby zastosować wybrany poziom zabezpieczeń, który najlepiej jest dopasowany do naszych potrzeb (zgodnie z opisem w tabeli powyżej):

1. Kliknij na wybrany poziomu ochrony zapory sieciowej.

Uwaga: Zastosowanie minimalnych ustawień zabezpieczeń zapory sieciowej może narazić sieć domową na znaczne ryzyko związane z bezpieczeństwem i atakiem, np. od strony Internetu, a zatem tryb ten powinien być stosowany wyłącznie, gdy jest to absolutnie konieczne i na krótki okres czasu.

2. Kliknij przycisk „OK", aby zapisać wybrane ustawienia.

Domyślnie wybrany poziom bezpieczeństwa wpływa na dostęp do takich usług, jak „Internet File Transfer Protocol" (FTP), przeglądanie stron WWW (HTTP i HTTPS), „Domain Name Sernice" (DNS), usługi e-mail (IMAP, POP3 i SMTP), dostęp do wiersza polecenia na komputerach zdalnych (Telnet).

Zauważ, że niektóre programy (takie jak niektóre komunikatory internetowe oraz oprogramowanie klienckie do wymiany plików P2P) mają tendencję do korzystania z wyżej wymienionych usług w przypadku, gdy nie mogą połączyć się za pomocą własnych domyślnych portów. Zezwalając na taką akcję, żądanie połączenia z Internetem przez takie

programy nie będzie mogło być blokowane, nawet gdy poziom bezpieczeństwa zostanie ustawiony jako „Maksymalne bezpieczeństwo".

Po wybraniu odpowiedniego poziomu zabezpieczeń, zapora sieciowa reguluje przepływ danych między siecią domową a Internetem. Przychodzące i wychodzące dane są kontrolowane według elastycznych reguł, a następnie akceptowane (mogą przechodzić przez OpenRG) lub odrzucone (zablokowane przez OpenRG). Przepisy te mają na celu zapobieganie niechcianym włamaniom z zewnątrz, jednocześnie umożliwiając użytkownikom domowym dostęp do usług internetowych.

Na przykład, gdy wpisujemy przykładowy adres w przeglądarce internetowej, żądanie zostanie wysłane do Internetu, następnie pobrane i strona zostanie załadowana. Gdy żądanie to przechodzi przez OpenRG, jego zapora sieciowa sprawdza żądanie, rodzaj i pochodzenie żądania. Dla przykładu w przypadku przeglądarki internetowej HTTP jest typem żądania, a komputer jest źródłem. Jeśli nie posiadamy skonfigurowanej kontroli dostępu w zaporze sieciowej OpenRG dla tego typu żądań pochodzących z danego komputera, zapora pozwala na to żądanie i dostęp do Internetu (więcej na temat konfiguracji kontroli dostępu w zaporze sieciowej OpenRG, patrz punkt 5.2.2).

Jeśli strona sieci www jest zwracana przez serwer www, zapora sieciowa skojarzy go z obecnym połączeniem i pozwoli przejść niezależnie od tego, czy dostęp HTTP z internetu do sieci domowej jest zablokowany lub dozwolony. Jest to źródło żądania, nie zaś późniejsza odpowiedź na to żądanie, które określa, czy można nawiązać połączenie, czy nie.

5.2.2. Kontrola dostępu do usług internetowych

Jeśli chcesz, możesz zablokować wybrane komputery w sieci domowej (lub nawet całej sieci), lub zablokować dostęp do niektórych usług dostępnych w Internecie. Na przykład, możesz zabronić jednemu komputerowi przeglądanie stron www, innemu komputerowi przesyłanie plików za pomocą FTP, a całej sieci dostępu do e-mail. Sekcja „Kontrola dostępu" umożliwia zastosowanie ograniczeń rodzaju żądanego połączenia, które może przejść z sieci domowej do Internetu i blokowania ruchu w sieci odpowiednio w obu

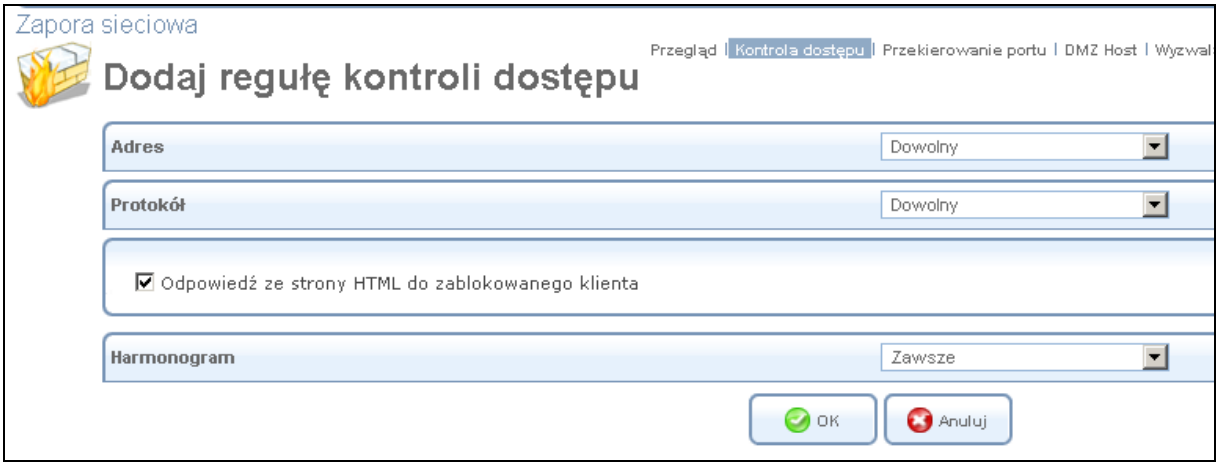
kierunkach. Ponadto sekcja ta może być stosowana w celu umożliwienia dostępu do określonych usług, jeżeli polityka bezpieczeństwa została określona jako „Maksymalne bezpieczeństwo" (jak opisano w punkcie 5.2.1).

• Aby zablokować dostęp do usług dostępnych w Internecie:

1. Kliknij link „Kontrola dostępu" w menu „Zapora sieciowa". Wygląd interfejsu „Kontrola dostępu".

Rysunek 5.4 Kontrola dostępu

2. Kliknij „Nowy wpis". Zostanie wyświetlone dodawanie reguły kontroli dostępu.



Rysunek 5.5 Dodawanie reguły kontroli dostępu

3. Z rozwijanego menu „Adres", wybierz adres IP lub nazwę komputera z listy w celu zastosowania tej reguły do odpowiedniego komputera w sieci LAN lub opcję „każdy", aby zastosować regułę na wszystkich komputerach w sieci LAN.
4. Z menu „Protokół" z rozwijanej listy wybierz typ protokołu używanego przez usługę. Należy pamiętać, że wybierając „Pokaż wszystkie usługi" opcja rozszerza listę dostępnych protokołów.

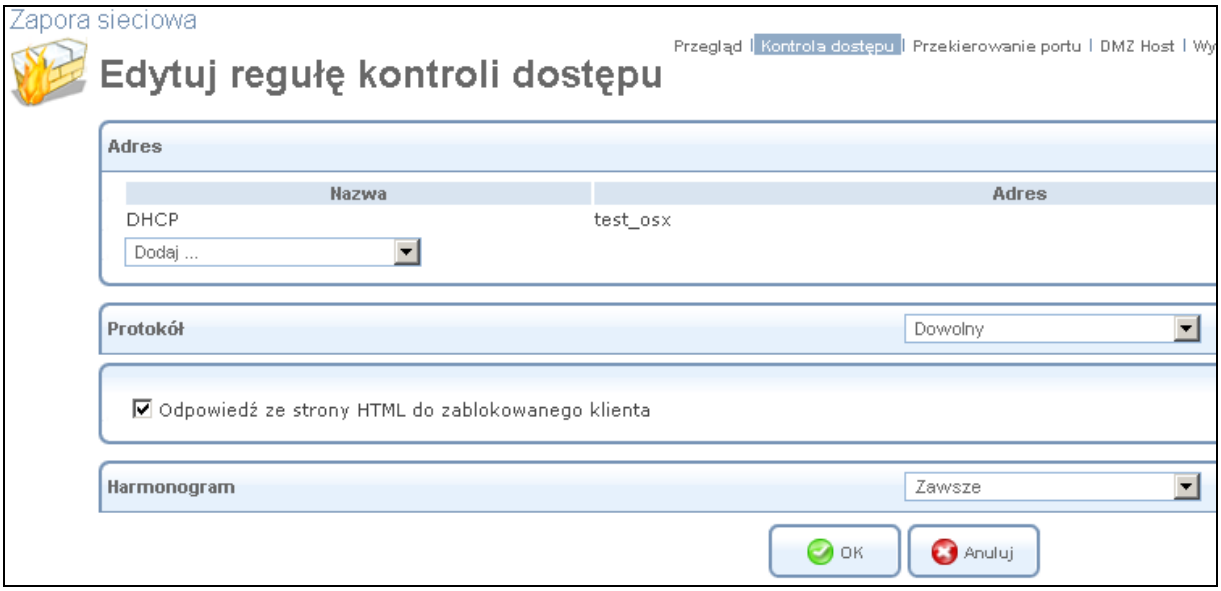
W przypadku wybrania protokołu HTTP i HTTPS (w celu odmowy dostępu do Internetu), można również włączyć funkcję „Odpowiedź ze strony HTML do zablokowanego klienta". Gdy to pole wyboru zostanie zaznaczone, następujący komunikat zostanie wyświetlony w przeglądarce zablokowane komputera w sieci LAN, gdy użytkownik próbuje korzystać z Internetu *„Dostęp zabroniony" - ten komputer nie może korzystać z Internetu, należy skontaktować się z administratorem*". Jeśli to pole wyboru nie jest zaznaczone, żądania połączenia z internetem są po prostu ignorowane i podany komunikat nie zostanie wyświetlony.

5. Domyślnie reguła będzie zawsze aktywna. Można jednak określić segmenty czasu, w którym reguły mogą być aktywne, wybierając opcję „Definiowane przez użytkownika" z rozwijanego menu sekcji „Harmonogram". Jeżeli więcej niż jeden wpis jest określony w harmonogramie, z rozwijanego menu możemy wybierać między dostępnymi regułami. Aby dowiedzieć się, jak skonfigurować reguły harmonogramu, odwołaj się do sekcji „Definiowanie reguł harmonogramu" w podręczniku administratora OpenRG.
6. Kliknij przycisk „OK", aby zapisać zmiany. Ekran „Kontrola dostępu" wyświetla podsumowanie dotyczące reguły, którą właśnie dodaliśmy.

Rysunek 5.6 Reguła kontroli dostępu

• Aby zmodyfikować wprowadzone reguły:

1. Kliknij ikonę „Działania”, następnie „Edytuj regułę kontroli dostępu”. Ta sekcja pozwala na edycję wszystkich parametrów, które skonfigurowano przy tworzeniu reguły kontroli dostępu.



Rysunek 5.7 Edycja reguły kontroli dostępu

Uwaga: Można określić dodatkowe komputery LAN i protokoły, które będą zablokowane przez zasady kontroli dostępu, wybierając je z rozwijanego menu „Dodaj ...”

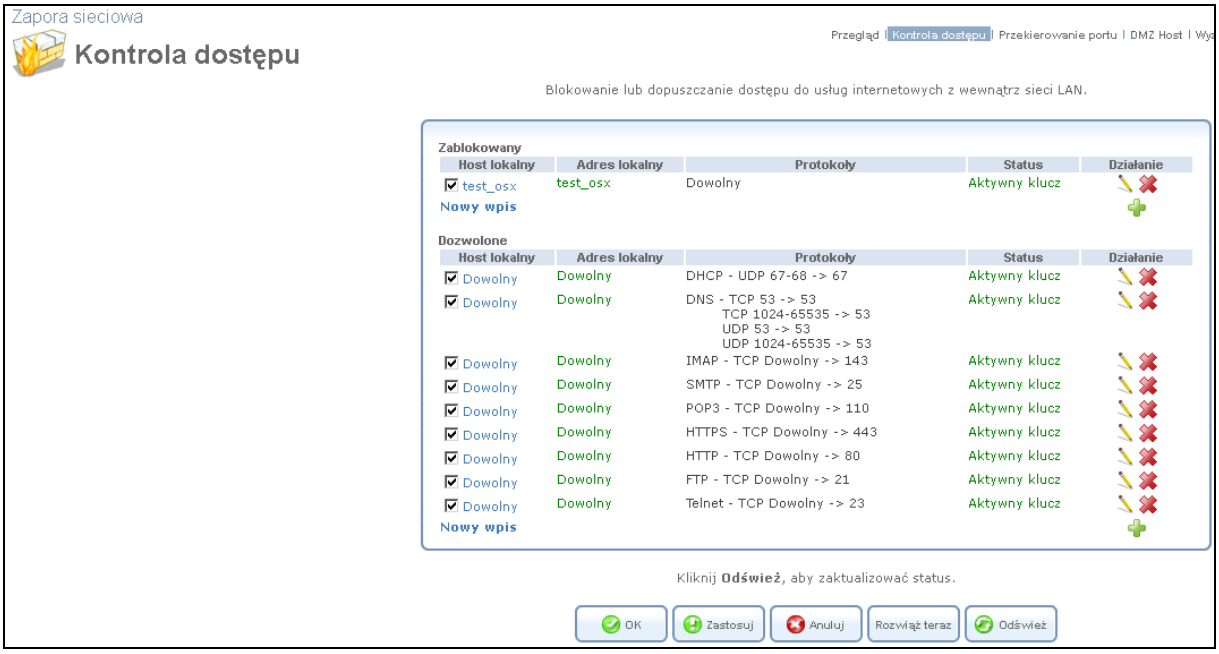
2. Kliknij przycisk „OK”, aby zapisać zmiany i powrócić do ekranu „Kontrola dostępu”. Można wyłączyć regułę kontroli dostępu w celu zapewnienia dostępu dla danej usługi, bez konieczności kasowania jej reguły z sekcji „Kontrola dostępu”. Funkcja ta może być przydatna, jeśli chcesz, aby odblokować dostęp do usługi tylko tymczasowo, chcąc jednak przywrócić ograniczenia w przyszłości.

• Aby tymczasowo wyłączyć regułę, wyczyść pole wyboru obok nazwy usługi.

• Aby przywrócić regułę w późniejszym czasie, po prostu ponownie należy wybrać pole wyboru.

• Aby usunąć regułę, kliknij ikonę „Usuń”. Reguła zostanie na stałe usunięta.

W przypadku, gdy wybrany mamy poziom „Maksymalne bezpieczeństwo”, sekcja „Kontrola dostępu” wyświetla listę automatycznie wygenerowanych reguł zapory, które pozwalają na dostęp do określonych usług internetowych z komputerów w sieci lokalnej, przez zdefiniowane porty.



Rysunek 5.8 Kontrola dostępu - dozwolone usługi w trybie maksymalnego bezpieczeństwa.

Można zarządzać wyświetlonymi zasadami kontroli dostępu, a także tworzyć nowe (umożliwiające dostęp do innych usług), jak opisano wcześniej w sekcji kontroli dostępu.

5.2.3. Zdalne łączenie się z siecią wewnętrzną i wykorzystanie funkcji przekierowania portów

Domyślnie, zapora sieciowa OpenRG blokuje wszystkich użytkowników zewnętrznych chcących połączyć się naszą siecią lokalną. Dlatego komputery podłączone do naszego urządzenia są zabezpieczone przed atakami hakerów, którzy mogą próbować włamać się do naszej sieci w celu jej uszkodzenia. Jednakże, możesz zezwolić na połączenia z sieci Internet do naszej sieci lokalnej w sposób ograniczony i kontrolowany. Funkcja „Przekierowanie portów” OpenRG pozwala to zrobić. Jeśli posiadasz znajomość terminologii i pojęć sieciowych, to być może spotkaliście się Państwo z funkcją „Przekierowania portów” nazwaną często jako „Serwery lokalne”.

Funkcja „Port Forwarding" umożliwia zdefiniowanie aplikacji (np. Peer-to-Peer, gier, vpn, czatów lub innych programów), które będą mogły uzyskać bezpośrednie połączenie z Internetem. Ponadto, można użyć funkcji przekierowania portów, aby umożliwić dostęp z zewnątrz do konkretnych serwerów działających w sieci wewnętrznej. Na przykład, jeśli chcesz, aby umożliwić dostęp z zewnątrz do serwera File Transfer Protocol (FTP)

działającego na PC w LAN, to po prostu należy utworzyć przekierowanie portów, które określa, że wszystkie przychodzące z zewnątrz do OpenRG dane związane z FTP będą odtąd przekazane do określonego komputera w sieci LAN.

Innym przykładem wykorzystania funkcji Port Forwarding jest posiadanie własnej witryny WWW na własnym serwerze. Gdy użytkownik z Internetu wpisuje w przeglądarce adres IP zewnętrzny OpenRG, brama przesyła przychodzące żądanie HTTP do serwera www w naszej sieci LAN, jeśli odpowiednie reguły przekierowania portów zostały ustalone.

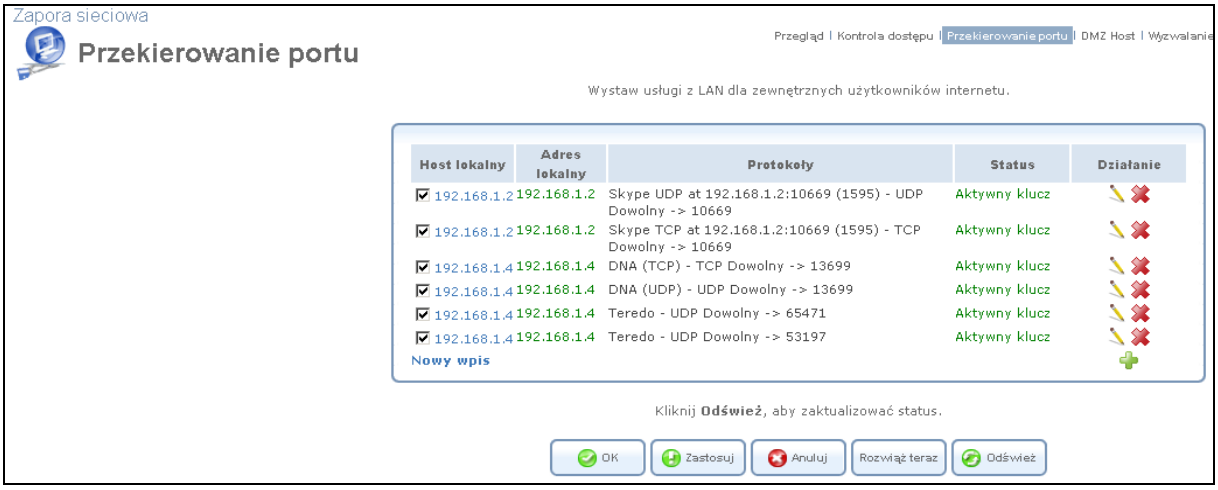
Dodatkowo, funkcja przekierowania portów OpenRG pozwala na przekierowanie ruchu do innego portu, a nie na ten port, który został wyznaczony. Na przykład, jeśli posiadamy serwer www na komputerze na porcie 8080, możesz przekierować każdego, kto przejdzie do zewnętrznego adresu IP OpenRG (domyślnie serwer www pracuje na porcie 80) na nasz serwer www. Aby dowiedzieć się, jak to zrobić, przejdź do sekcji 5.2.3.2.

Uwaga: Usługi zdalnej administracji będą miały pierwszeństwo przed regułami przekierowania portów stworzonych na lokalnym serwerze, gdy obie reguły są skonfigurowane do korzystania z tego samego portu. Na przykład, gdy zarówno serwer www (działa w sieci LAN na hoscie) i usługa zdalnej administracji (wykorzystywana przez ISP) jest skonfigurowana do korzystania z portu 80, OpenRG pozwoli na uzyskanie dostępu do sieci zdalnej administracji. Ruch przeznaczony dla serwera www zostanie zablokowany do czasu wyłączenia usługi zdalnej administracji lub możemy zmienić jej dedykowany port. Aby uzyskać więcej informacji na temat usługi administracji zdalnej, zobacz rozdział 6.7.2.

5.2.3.1. Dodanie reguły przekierowania portów

Aby umożliwić zdalny dostęp do usług na jednym z komputerów w sieci LAN, tworzenie reguły dla odpowiedniego portu przeprowadzamy w następujący sposób:

1. Kliknij przycisk „Przekierowanie portu" w menu „Zapora sieciowa". Ekran „Przekierowanie portu" wygląda następująco:



Rysunek 5.9 Interfejs przekierowania portu

2. Kliknij „Nowy wpis", zostanie wyświetlony interfejs dodawania reguły przekierowania portu.

Rysunek 5.10 Proste dodawanie reguły przekierowania portu

3. Wybieramy opcję „Host lokalny" z rozwijanego menu, wyświetlona zostanie lista dostępnych komputerów sieci LAN. Wybierz komputer, dla którego utworzona zostanie reguła przekierowania portu.
4. Z rozwijanego menu „Protokół" wybierz typ protokołu używanego przez usługę. Uwaga: Wybierając „Pokaż wszystkie usługi" wyświetlona zostanie rozszerza lista dostępnych protokołów.
5. Kliknij przycisk „Zaawansowane" na dole ekranu. Po odświeżeniu ekranu, wyświetlanie zostaną dodatkowe opcje „Przekaż do poru" i „Harmonogram".

Rysunek 5.11 Zaawansowane dodawanie reguły przekierowania portu

Podczas tworzenia reguły przekierowania portu, należy upewnić się, że port wykorzystywany przez wybrany protokół nie jest już używany przez inne Państwa usługi lokalne, które w tym przypadku, mogą uniemożliwić poprawne funkcjonowanie reguły przekierowania portów.

6. Domyślnie OpenRG przekazuje ruch do tego samego portu, co port połączeń przychodzących. Jeśli chcesz przekierować ruch do innego portu, wybierz opcję „Określ" z „Przekieruj do portu" z rozwijanego menu. Po odświeżeniu ekranu, pojawi się dodatkowe pole, pozwalające na podanie numer portu.

Rysunek 5.12 Przekieruj do określonego portu

7. Domyślnie reguła będzie zawsze aktywna. Można jednak określić czas aktywności reguły, czas gdy reguła będzie aktywna możemy określić, wybierając opcję „Definiowane przez użytkownika" z rozwijanego menu harmonogramu. Jeżeli więcej niż jedna reguła jest określona w harmonogramie, z rozwijanego menu możemy wybrać pomiędzy dostępnymi regułami. Aby dowiedzieć się, jak skonfigurować harmonogram reguł, możemy zobaczyć w sekcji „Definiowanie reguł harmonogramu" instrukcji administracyjnej OpenRG.

8. Kliknij przycisk „OK.”, aby zapisać ustawienia. Ekran przekierowania portu wyświetli podsumowanie reguły, którą właśnie dodaliśmy.

Rysunek 5.13 Reguły przekierowania portów

Możesz edytować reguły przekierowania portów, klikając na jego pozycję w kolumnie „Host lokalny” w sekcji „Przekierowanie portu”. Można także wyłączyć określone reguły w celu uniemożliwienia dostępu do danego portu w sieci LAN bez konieczności kasowania reguły z sekcji „Przekierowanie portu”. Funkcja może być przydatna, jeśli chcesz, aby usługa niedostępna była tylko tymczasowo, zamierzasz przywrócić usługę w przyszłości.

• Aby tymczasowo wyłączyć regułę, wyczyść pole wyboru obok nazwy usługi.
• Aby przywrócić regułę w późniejszym czasie, należy po prostu ponownie wybrać pole wyboru.
• Aby usunąć regułę, kliknij ikonę „Usuń”. Serwis będzie stale usunięty.

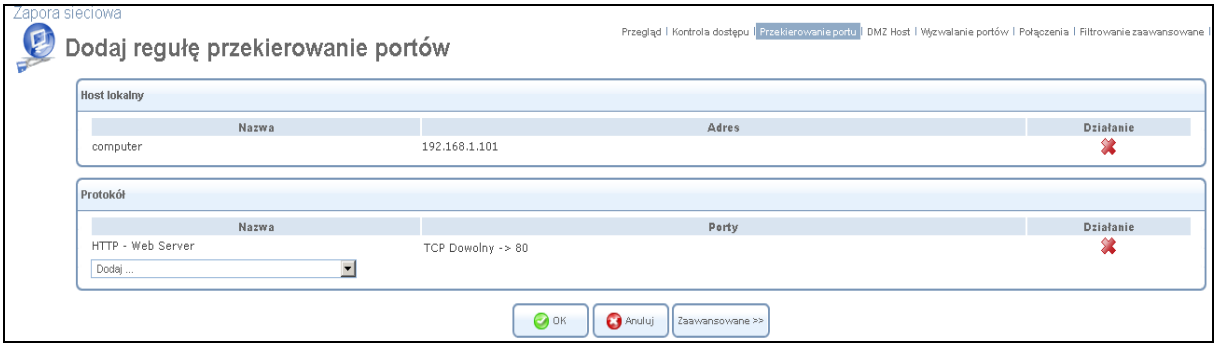
Wszystkie komputery w sieci lokalnej mogą jednocześnie korzystać z określonej usługi w charakterze klientów. Bycie klientem oznacza, że komputer w sieci inicjuje połączenie, np. otwiera połączenie FTP z serwerem FTP w Internecie. Jednakże tylko jeden komputer może służyć jako serwer i odpowiedzi na żądania komputerów z Internetu .

5.2.3.2 Przykład przekierowania portu

W celu umożliwienia dostępu z zewnątrz (z Internetu) do serwera wewnątrz sieci LAN, należy skonfigurować zaporę sieciową OpenRG, dodając regułę przekierowania portu. Poniższy przykład demonstruje jak utworzyć regułę przekierowania portu, która przekierowuje wszystkich użytkowników zdalnych do lokalnego serwera www działającego na porcie 8080, gdy użytkownik z Internetu wpisze w przeglądarce nasz zewnętrzny adres IP OpenRG.

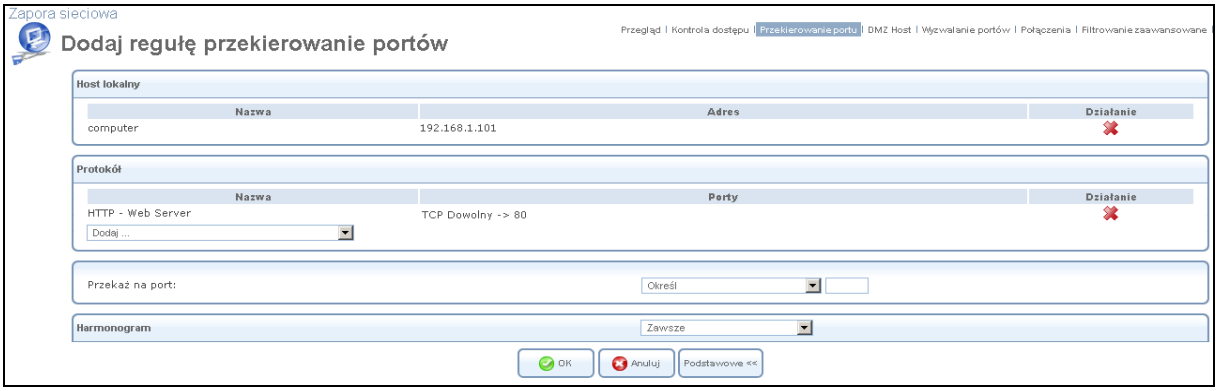
Aby zdefiniować taką regułę przekierowanie portu, wykonaj następujące czynności:

1. W sekcji OpenRG „Przekierowanie portu", kliknij przycisk „Nowy wpis". Poniżej widzimy interfejs „Dodaj regułę przekierowania portu".



Rysunek 5.14 Dodanie reguły przekierowania portu

2. Z rozwijanego menu „Host lokalny" wybierz nazwę komputera lub adres IP, na którym jest zainstalowany serwer www. W menu „Protokół" z rozwijanego menu, wybierz protokół „HTTP". Ekran odświeża się po każdej zmianie parametrów.
3. Kliknij przycisk „Zaawansowane" na dole ekranu. Po odświeżeniu ekranu, z rozwijanego menu wybierz „Przekieruj do portu".



Rysunek 5.15 Zaawansowane przekierowanie portu

4. Wybierz „Określ" z rozwijanego menu i wpisz port „8080" jak na ekranie poniżej.

Rysunek 5.16 Przekieruj do portu 8080

5. Kliknij przycisk „OK.", aby zapisać wprowadzone ustawienia.
6. Aby sprawdzić, czy przekierowanie portów działa poprawnie, wpisz zewnętrzny adres IP OpenRG w przeglądarce zdalnego komputera. Powinieneś zostać przekierowany do serwera www działającego w sieci lokalnej. Możesz wyłączyć regułę przekierowania portu poprzez odznaczenie przy polu wyboru w sekcji „Przekierowanie portu". Wtedy jeśli chcemy uzyskać połączenie z lokalnym serwerem www z Internetu, połączenie z serwerem www nie będzie dostępne.

5.2.4. Wyznaczenie hosta DMZ

DMZ (strefa zdemilitaryzowana) funkcja pozwalająca jednego hosta z lokalnych komputerów wystawiać do sieci Internet. Używamy funkcji DMZ, gdy:

• Chcesz użyć usługi internetowej specjalnego przeznaczenia, takie jak gry on-line, program do video konferencji lub jeśli nie znamy portu usługi, która wymaga bezpośredniego połączenia z Internetem i nie występuje na liście w sekcji „Przekierowanie portu".

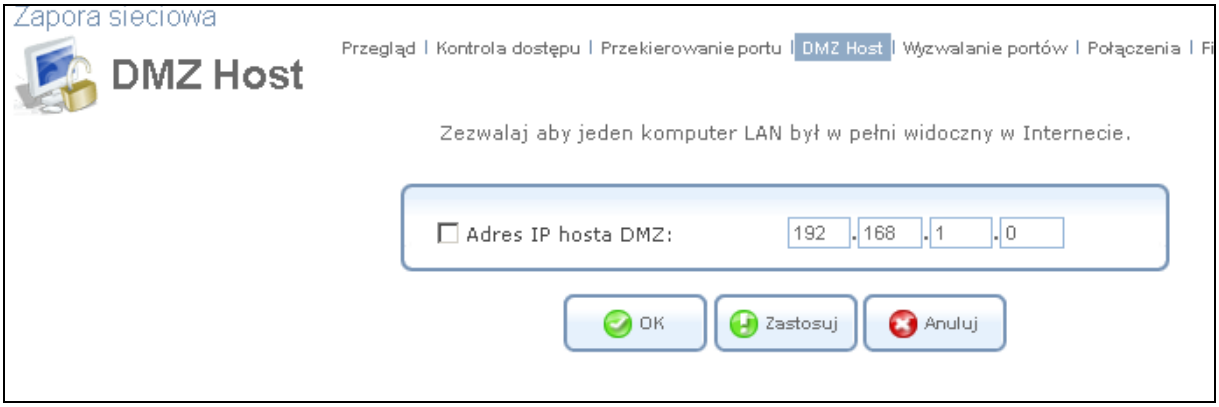
• Host, który umieścimy w DMZ będzie narażony na ataki z sieci Internet, jeden komputer ze wszystkimi usługami bez ograniczeń będzie dostępny z Internetu.

Uwaga: DMZ nie jest chroniony przez zaporę sieciową i może być podatny na ataki. Wykorzystanie funkcji DMZ może również zmniejszyć bezpieczeństwo innych komputerów w sieci domowej. Przy wykorzystaniu DMZ, należy uwzględnić wpływ na bezpieczeństwo i zwiększyć ochronę na komputerach w sieci lokalnej.

Przychodzące żądanie dostępu do usługi w sieci domowej, takie jak dostęp do serwera www, który jest wystawiany przez OpenRG za pomocą funkcji DMZ. OpenRG przekazuje żądanie do hosta DMZ, jeżeli jest wyznaczony, chyba że usługa jest świadczona przez inny komputer w naszej sieci LAN (zdefiniowany w regule umieszczonej w sekcji „Przekierowanie portu"), w którym to przypadku komputer posiadający wpis w sekcji „Przekierowanie portu" otrzyma dane żądanie.

• Aby wyznaczyć lokalnego komputer jako host DMZ:

1. Kliknij przycisk „DMZ Host" w menu „Zapora sieciowa". Interfejs „DMZ Host" wygląda, jak poniżej.



Rysunek 5.17 Host DMZ

2. Zaznacz pole wyboru i wprowadź lokalny adres IP komputera, który chcesz wyznaczyć jako host DMZ. Należy pamiętać, że tylko jeden komputer z sieci LAN może być wykorzystany jako host DMZ w dowolnym momencie.

3. Kliknij przycisk „OK”, aby zapisać wprowadzone ustawienia.

• Można wyłączyć DMZ tak, że host nie będzie widoczny w Internecie, a jego adres IP zostanie zapisany w sekcji „DMZ Host”. Aby to zrobić, wyczyść pole wyboru obok pola „Adres IP hosta DMZ”, a następnie kliknij „OK.”. Może to być przydatne, jeśli chcesz, aby tymczasowo wyłączyć DMZ, chcąc włączyć go ponownie w przyszłości.
• Aby przywrócić go na później, ponownie wybierz pole wyboru i kliknij „OK.”.

5.2.5. Korzystanie z funkcji wyzwalania portów

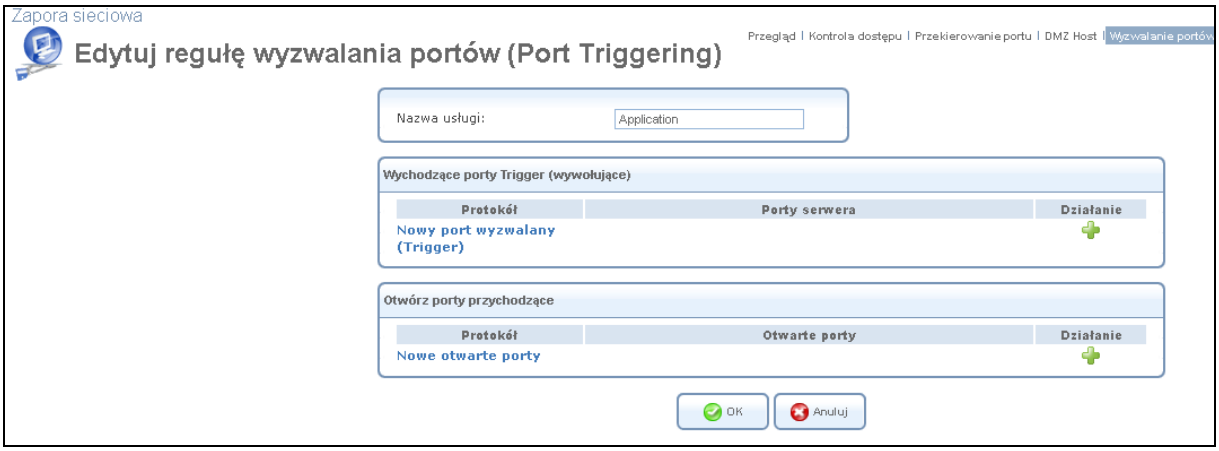
Funkcja wyzwalania portów (Port Triggering) służy do ustawiania dynamicznej konfiguracji przekierowywania portów. Po ustawieniu reguł wyzwalania portu, możemy zezwolić na ruch przychodzący, aby dotarł z zewnątrz do określonego hosta w sieci LAN, wykorzystując porty inne niż te używane przy ruchu wychodzącym. Określamy to wyzwalaniem portów od wyzwalanego ruchu wychodzącego do których portów jest skierowany ruch przychodzący.

Rozważmy na przykład serwer gry, który jest dostępny poprzez protokół UDP na porcie 2222. Serwer gry reaguje po podłączeniu użytkownika za pomocą UDP na porcie 3333, po rozpoczęciu sesji gry. W takim przypadku należy użyć wyzwalania portów, ponieważ koliduje to z następującymi domyślnymi ustawieniami zapory sieciowej:
• Zapora sieciowa blokuje domyślnie ruch przychodzący.
• Odpowiedź serwera na IP OpenRG, a połączenie nie jest odsyłane z powrotem do hosta, ponieważ nie jest częścią sesji.
Aby rozwiązać ten problem, należy określić wyzwalany port wejścia, co pozwala na połączenie na porcie UDP 3333 tylko, gdy host sieci LAN wygenerował ruchu do portu UDP 2222. Aby to zrobić, wykonaj następujące czynności:

1. Kliknij na link „Wyzwalanie portów” w menu „Zapora sieciowa”. Ekran „Wyzwalanie portów” wyświetli sekcję, jak poniżej. Wyświetlone zostaną wszystkie wpisy wyzwalanych portów.

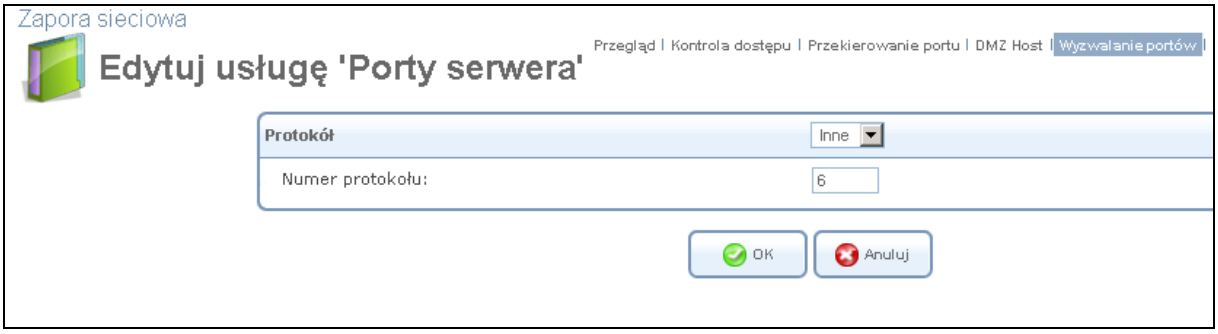
Rysunek 5.18 Wyzwalanie portów

4. Wybierz opcję „Definiowane przez użytkownika”, aby dodać wpis. Ekran „Edytuj regułę wyzwalania portów” poniżej.



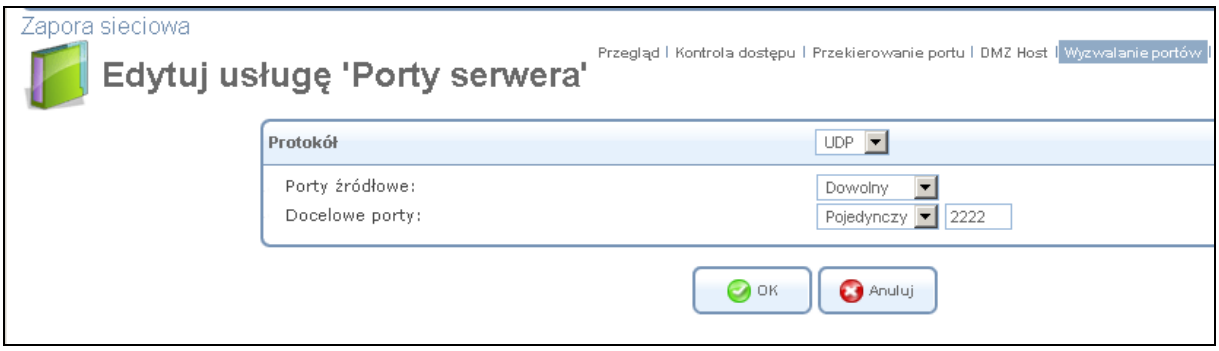
Rysunek 5.19 Edytuj regułę wyzwalania portów

5. Wpisz nazwę usługi (np. „serwer_gry”) i kliknij link „Nowy wyzwalany port”. Ekran „Edytuj usługę 'Porty serwera'” poniżej.



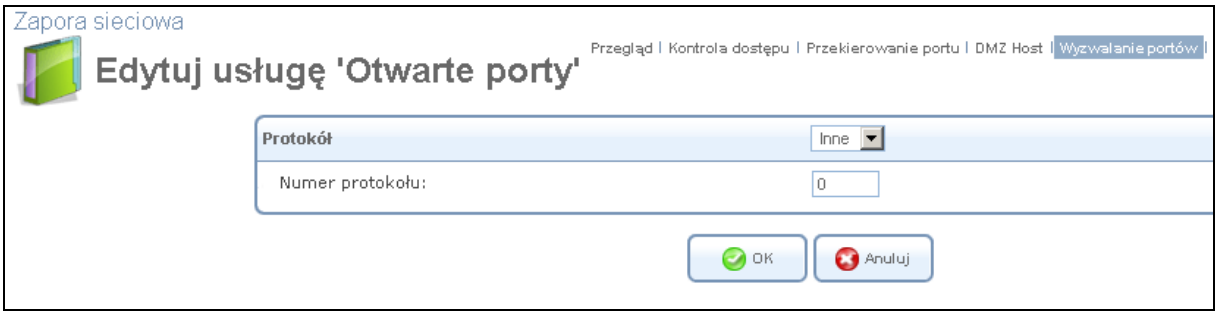
Rysunek 5.20 Edytuj usługę „Porty serwera”

6. Z rozwijanego menu „Protokół”, wybierz opcję „UDP”. Ekranie zostanie odświeżony, wyświetlając opcje źródłowego i docelowego portu (patrz rysunek 5.21).
7. Z menu rozwijanej listy „Port źródłowy” domyślnie wybrana jest opcja „Dowolny”. Z opcji „Port docelowy” rozwijanego menu, wybierz „Pojedynczy”. Ekran zostanie ponownie odświeżony, zapewniając dodatkowe pole, w które należy wpisać port przeznaczenia „2222”.



Rysunek 5.21 Edycja usługi portów serwera

8. Kliknij przycisk „OK.”, aby zapisać ustawienia.
9. Wracamy do sekcji „Edycja reguły wyzwalanego poru” (Rysunek 5.19), kliknij link „Nowy otwarty port”. Wyświetlony zostanie ekran „Edytuj usługę otwartych portów”.

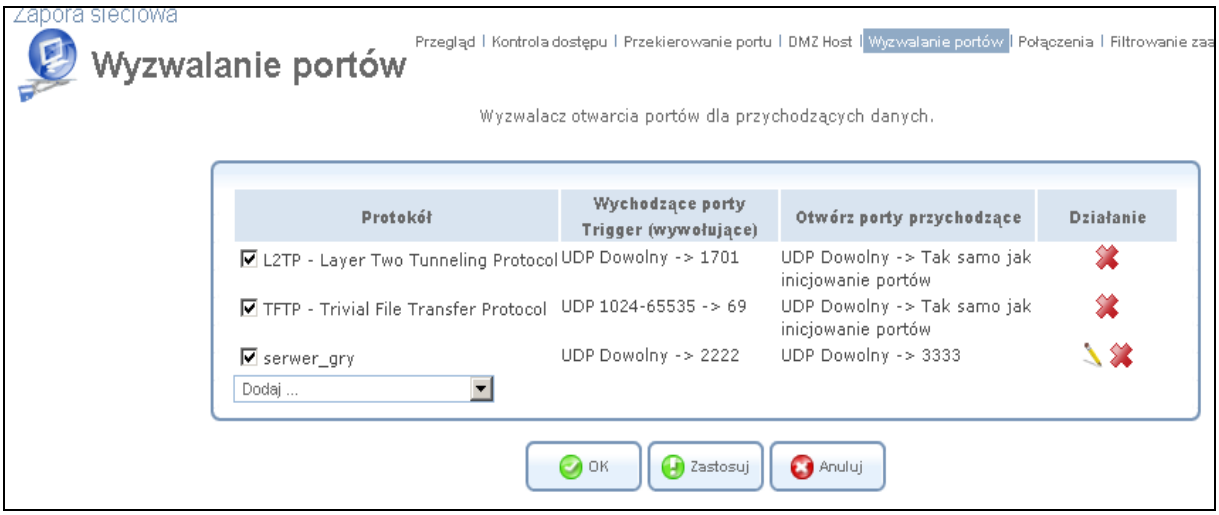


Rysunek 5.22 Edytuj usługę otwartych portów

10. Wybierz UDP jako protokół, pole port źródłowy pozostaw jako „Dowolny” i jako port docelowy wybierz „Pojedynczy” i wpisz „3333”.

Rysunek 5.23 Edytuj usługę otwartych portów

11. Kliknij przycisk „OK", aby zapisać ustawienia. Ekran „Edycja usługi" prezentuje wprowadzone informacje. Kliknij przycisk „OK", aby zapisać zasady wyzwalania portów. Ekran „Wyzwalanie portów" zawiera nowy wpis wyzwalanego portu.



Rysunek 5.24 Nowa reguła portu wywołującego

To spowoduje zaakceptowanie przychodzącego ruchu z serwera gier i wysyłanie go z powrotem do hosta LAN, który zapoczątkował ruch wychodzący do portu UDP 2222.

• Aby tymczasowo wyłączyć regułę, wyczyść pole wyboru obok nazwy usługi.

• Aby przywrócić regułę w późniejszym czasie, należy po prostu ponownie wybrać pole wyboru.

• Aby usunąć regułę, kliknij ikonę „Usuń". Usługą zostanie na stałe usunięta.

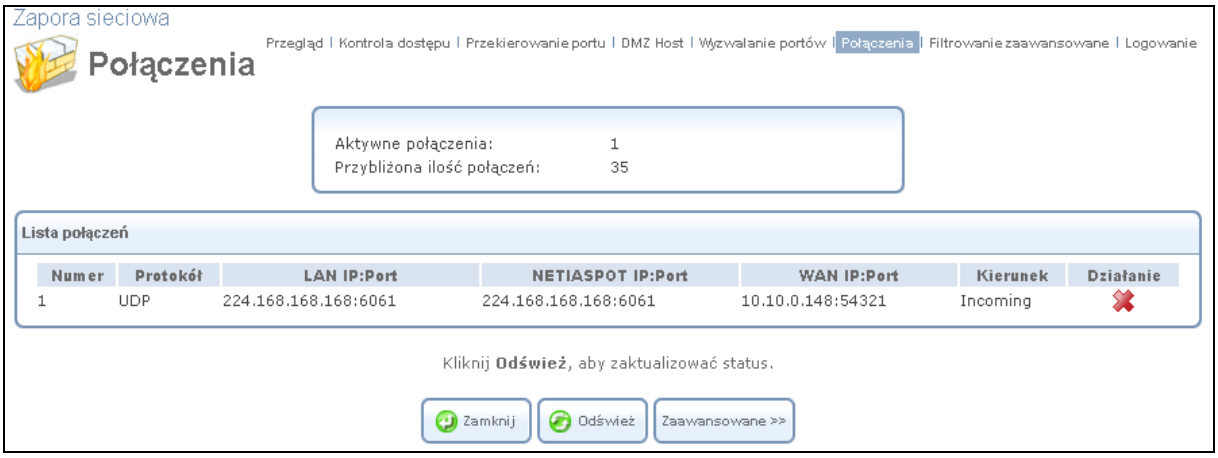
Uwaga: Może być kilka domyślnych reguł portów wywołujących przed dodaniem naszej własnej pierwszej reguły wyzwalania portów. Wyłączenie tych już istniejących reguł może spowodować zaburzenia funkcjonalności naszego urządzenia.

5.2.6. Przegląd otwartych połączeń

W sekcji „Połączenia" wyświetlane są wszystkie połączenia, które są obecnie otwarte, jak również odpowiadające im dane i statystyki. Podsumowanie na górze ekranu pokazuje liczbę aktywnych połączeń, a „Przybliżona ilość połączeń", oznacza ilość dodatkowych jednoczesnych możliwych połączeń.

Gdy liczba dostępnych jest wiele połączeń, możemy kliknąć „Połączeń na stronie" z menu rozwijanego w prawym dolnym rogu wybieramy ilość widocznych w tabeli połączeń.

Główne menu składa się z nazwy protokołu, wykorzystywane porty i kierunek, w którym połączenie zostało zainicjowane.



Rysunek 5.25 Lista połączeń

Aby usunąć niepożądaną połączenie, kliknij na jego ikonę w menu „Działanie" i „Usuń". Kliknięcie przycisku „Zaawansowane" w dole tabeli wyświetla następujące dane:

• Czas życia połączenia

• Liczba kilo-bajtów, pakietów otrzymanych i przekazanych

• Typ urządzenia

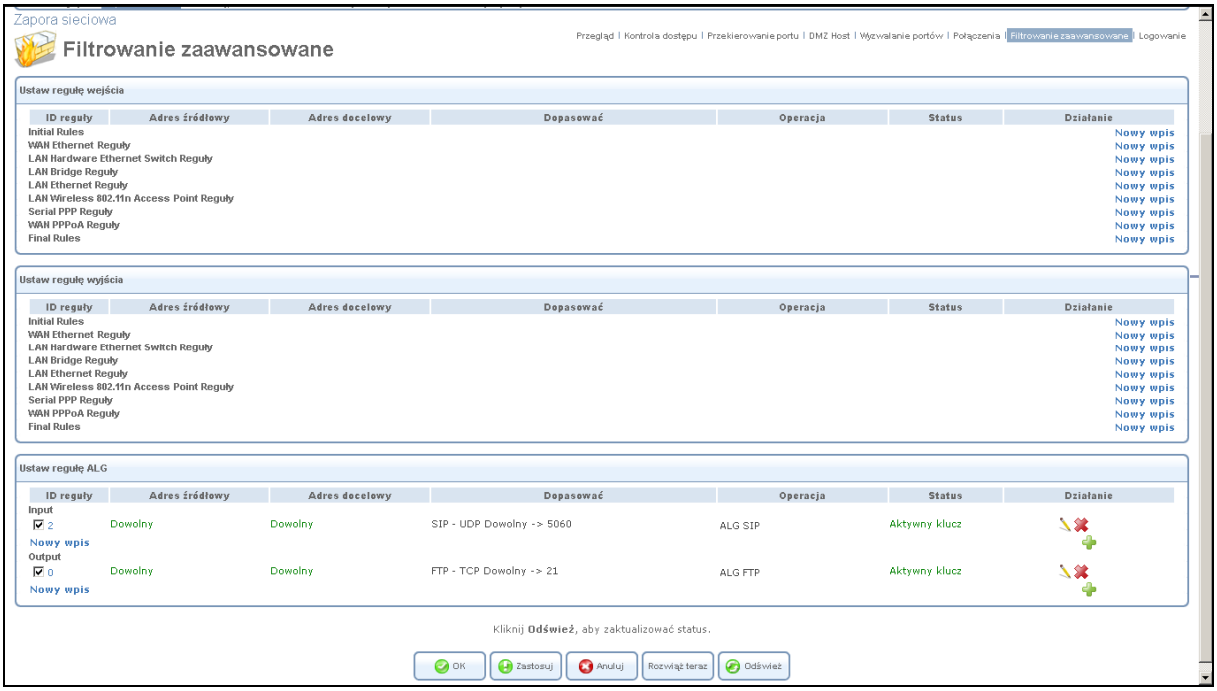
• Tryb trasowania

Zauważ, że pole protokołu może zawierać „nieokreślone połączenia", które pojawiają się w postaci gwiazdek ('*') (patrz rys. 5.25). Nieokreślone połączenia są tworzone, gdy adres IP lub port źródłowy, pakiet przychodzący nie są znane. Gdy pakiet pasuje do połączenia, brakujące szczegóły zostaną ujawnione, w wyniku standardowego połączenia.

5.2.7. Konfiguracja mechanizmu zaawansowanego filtrowania

Zaawansowane filtrowanie zaprojektowano w sposób umożliwiający pełną kontrolę nad zachowaniem zapory sieciowej. Możemy określić szczegółowe reguły wejścia i wyjścia, kontrole kolejności logicznie podobnych zestawów reguł i rozróżnić reguły mające zastosowanie do urządzeń WAN i LAN.

Aby wyświetlić zaawansowane opcje filtrowania OpenRG, należy kliknąć link „Zaawansowane filtrowanie" w sekcji menu „Zapora sieciowa". Ekran „Zaawansowane filtrowanie" wygląda, jak poniżej.



Rysunek 5.26 Zaawansowane filtrowanie

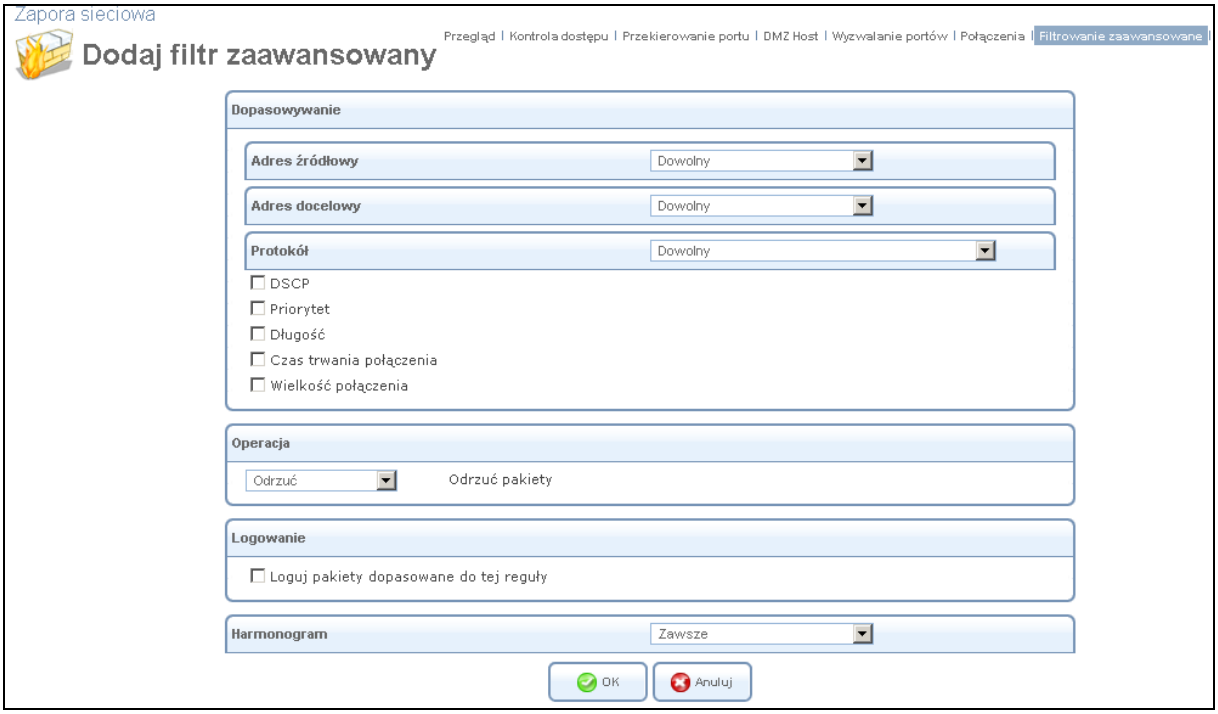
5.2.7.1 Dodawanie reguł wejściowych i wyjściowych

Pierwsze dwie części sekcji „Filtrowanie zaawansowane", dzieli się na zestaw reguł wejścia i wyjścia. Reguły te są przeznaczone do konfigurowania ruchu odpowiednio przychodzącego i wychodzącego. Każda sekcja składa się z podzbiorów, które można podzielić na trzy główne typy:

• Reguły wstępne - reguły określone tutaj będą stosowane jako pierwsze, na wszystkich urządzeniach bramy.
• Reguły urządzeń sieciowych - reguły mogą być określone na każdym urządzeniu bramy.
• Reguły końcowe – reguły określone tutaj będą stosowane ostatnie, na wszystkich urządzeniach bramy.

Istnieje wiele reguł, które są tworzone automatycznie przez zaporę sieciową w celu zapewnienia poprawy bezpieczeństwa i blokowania szkodliwych ataków.

Aby dodać zaawansowane reguły filtrowania, najpierw należy wybrać kierunek ruchu sieciowego oraz urządzenia, na których można ustawić reguły. Następnie kliknij na link „Nowy wpis". Wyświetlony zostanie ekran „Dodaj filtr zaawansowany".



Rysunek 5.27 Dodaj filtr zaawansowany

Sekcje menu „Dopasowanie" i „Operacja" określają działania, które zostaną wykonane, podczas gdy dopasowany pakiet zostanie rozpoznany.

Dopasowanie - w tej sekcji określamy cechy pakietów pasujących do danej reguły.

• **Adres źródłowy** pakietów wysyłanych lub otrzymywanych przez OpenRG. Użyj tej rozwijanej listy menu, aby określić komputer lub grupę komputerów, na których chcesz zastosować dane reguły. Wybierz adres lub nazwę z listy, aby zastosować regułę dla odpowiednich hostów lub „Dowolny", aby zastosować regułę na dowolnym komputerze próbującym wysłać dane. Jeśli chcesz dodać nowy adres, wybierz opcję „Zdefiniowane przez użytkownika" z rozwijanego menu. Wtedy rozpocznie się sekwencja, która doda obiekt sieciowy, reprezentujący nowego hosta.

• **Adres docelowy** to adres docelowy pakietów wysyłanych lub otrzymywanych przez OpenRG. Adres może być skonfigurowany w taki sam sposób, jak adres źródłowy. Na przykład, użyj rozwijanego menu, aby określić adres IP zdalnego serwera aplikacji (np. serwera bezpieczeństwa), który wymaga, aby przychodzące pakiety posiadały konkretny adres IP (np. jeden ze zdefiniowanych w puli adresów IP NAT).

• **Protokół** określa protokół ruchu sieciowego. Wybierz opcję „Pokaż wszystkie usługi" z rozwijanego menu, wtedy zostanie wyświetlona rozszerzona lista dostępnych protokołów. Wybierz protokół lub dodaj nowy, korzystając z opcji „Zdefiniowany przez użytkownika". Rozpoczniemy sekwencję, która doda usługę, reprezentującą protokół.

• **DSCP** - zaznacz pole wyboru, aby wyświetlić dwa pola DSCP, które umożliwiają określenie szesnastkowej wartości DSCP i jego maski przypisanej do pakietów pasujących do reguły pierwszeństwa.

• **Długość** to pole wyboru, jeśli go zaznaczymy, możemy określić długość pakietów, lub długości części ich danych.

• **Czas trwania połączenia** - zaznacz to pole wyboru, aby zastosować regułę filtrowania tylko dla połączeń, które są otwarte przez pewien okres czasu. Po zaznaczeniu pola wyboru, należy zdecydować, czy czas trwania połączeń pasujące do reguły i może być większy lub mniejszy niż czas, który można określić w sąsiednim polu.

Rysunek 5.28 Czas trwania połączenia

• **Wielkość połączenia** - zaznacz to pole wyboru, aby zastosować regułę filtrowania tylko dla połączeń pasujących do pewnej wielkości limitu danych. Tę opcję najlepiej jest stosować wraz z opcją „Czas trwania połączenia", co pozwala dostosować mechanizm filtrowania w zależności od potrzeb. Po wybraniu pola wyboru, należy zdecydować, czy rozmiar danych połączenia powinien być większy lub mniejszy niż liczba kilobajtów, które można określić w sąsiednim polu.

Rysunek 5.29 Wielkość połączenia

Operacja - definiuje, jakie działania zostaną podjęte odnośnie reguły, wybierając jedną z następujących akcji:

• **Odrzuć bez informacji zwrotnej**, odmowa dostępu do pakietów, które pasują do reguły źródłowego i docelowego adresu IP, usługi portów określonych powyżej.

• **Odrzuć z informacją zwrotną**, odmowa dostępu do pakietów, które spełniają określone kryteria i wysyła błąd ICMP lub TCP reset do właściciela odrzuconego pakietu.

• **Akceptuj połączenie**, zezwalaj na dostęp do pakietów, które spełniają określone kryteria. Dane sesji przesyłane będą za pomocą „Stateful Packet Inspection" (SPI), co oznacza, że inne pakiety pasujące do tej reguły będą posiadać automatycznie dostęp.

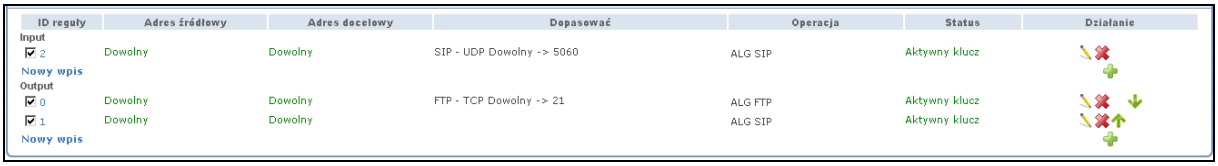
• **Akceptuj pakiet**, zezwalaj na dostęp do pakietów, które spełniają określone kryteria. Transfer danych sesji nie będzie obsługiwany przy użyciu SPI, co oznacza, że inne pakiety pasujące do tej reguły nie będą posiadały automatycznego dostępu. Funkcja może być przydatna, na przykład przy tworzeniu reguł, które umożliwiają nadawanie.

Logowanie, monitor reguły

• **Loguj pakiety dopasowane do tej reguły**, zaznacz to pole wyboru, aby zalogować pierwszy pakiet z połączenia, które zostało dopasowane do tej reguły.

Harmonogram, domyślnie reguła będzie zawsze aktywna. Można jednak określić czas segmentów, w którym reguły mogą być aktywne, wybierając opcję „Definiowane przez użytkownika" z rozwijanego menu. Jeżeli więcej niż jedna reguła jest określona, harmonogram z rozwijanego menu pozwala na możliwość wyboru między dostępnymi regułami. Aby dowiedzieć się, jak skonfigurować harmonogram reguł, odnieś się do „Określenie reguł harmonogramu" w części administracyjnej instrukcji OpenRG.

Kolejność pojawiania się reguły stanowi zarówno kolejność, w jakiej zostały one określone i sekwencję, w których będą stosowane. Możesz zmienić tę kolejność już po zdefiniowaniu reguł (bez konieczności kasowania, a następnie ponownie je dodać), za pomocą ikon(strzałka - góra, dół)



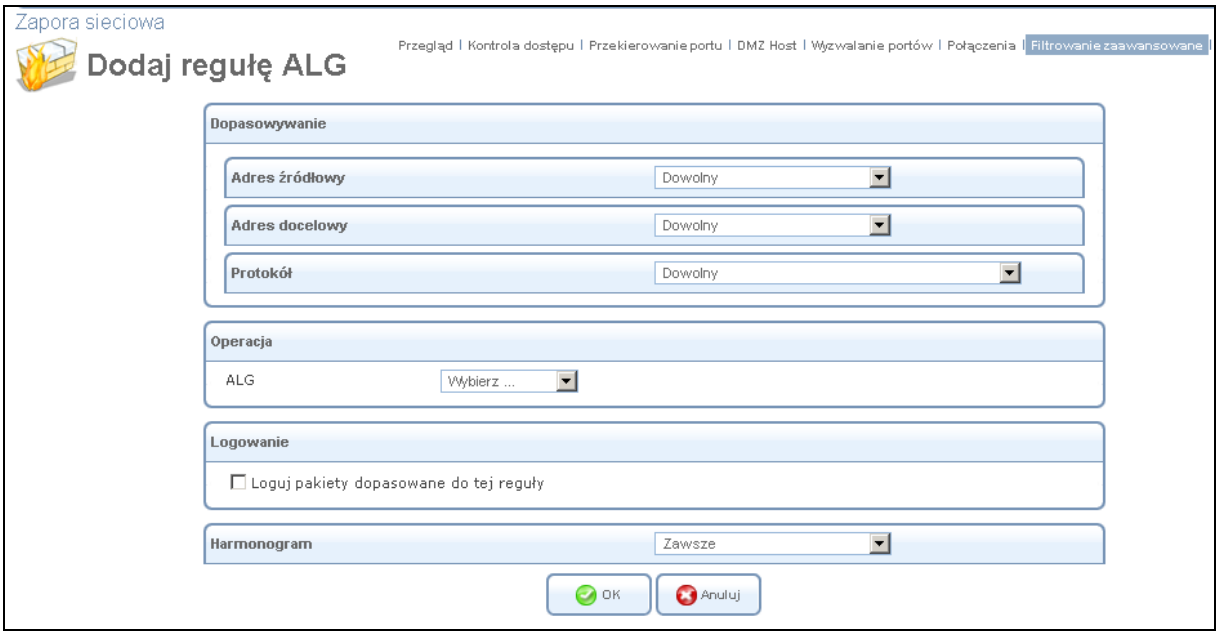
Rysunek 5.30 Ikony akcji (góra, dół)

5.2.7.2 Dodawanie reguły ALG

Sekcja „Dodaj regułę ALG" umożliwiającą zdefiniowanie adresu i portu przetwarzania w odniesieniu do niektórych protokołów aplikacji (takich jak, FTP, TFTP, SIP, i inne), które posiadają adres IP wewnątrz danych aplikacji. Większość z tych protokołów nie będzie działać z NAT, chyba że NAT jest poinformowany i wykona odpowiednie tłumaczenie.

NAT jest aplikacją niezależną, a więc dlatego jest wymagana brama poziomu aplikacji „Application Level Gateway" (ALG) aby umożliwić aplikacji na przekazywanie ruchu przez zaporę sieciową. Wejście i wyjście podsekcji ustawiania reguł ALG (patrz rysunek 5.26) przeznaczone są do wyświetlenia reguł ALG dla odpowiednio ruchu przychodzącego i wychodzącego. Należy pamiętać, że OpenRG jest automatycznie konfigurowany z zasadami ALG dla kilku powszechnych protokołów. Możesz edytować regułę, klikając na odpowiednią ikonę działania, lub usunąć klikając ikonę „Usuń".

W celu utworzenia reguły ALG, zarówno dla ruchu przychodzącego i wychodzącego, kliknij link „Nowy wpis", który odpowiada za rodzaj reguły, który chciałbyś zdefiniować. Ekran „Dodaj regułę ALG" wygląda, jak poniżej.



Rysunek 5.31 Dodanie reguły ALG

Sekcje menu „Dopasowanie" i „Operacja" określają działania, które zostaną wykonane podczas gdy dopasowany pakiet zostanie rozpoznany.

Dopasowanie - w tej sekcji określamy cechy pakietów pasujących do danej reguły.

• **Adres źródłowy** pakietów wysyłanych lub otrzymywanych przez OpenRG. Użyj tej rozwijanej listy menu, aby określić komputer lub grupę komputerów, na których chcesz zastosować dane reguły. Wybierz adres lub nazwę z listy, aby zastosować regułę dla odpowiednich hostów lub „Dowolny", aby zastosować regułę na dowolnym komputerze próbującym wysłać dane. Jeśli chcesz dodać nowy adres, wybierz opcję „Zdefiniowane przez użytkownika" z rozwijanego menu. Wtedy rozpocznie się sekwencja, która doda obiekt sieciowy, reprezentujący nowego hosta.
• **Adres docelowy** to adres docelowy pakietów wysyłanych lub otrzymywanych przez OpenRG. Adres może być skonfigurowany w taki sam sposób, jak adres źródłowy. Na przykład, użyj rozwijanego menu, aby określić adres IP zdalnego serwera aplikacji (np. serwera bezpieczeństwa), który wymaga, aby przychodzące pakiety posiadały konkretny adres IP (np. jeden ze zdefiniowanych w puli adresów IP NAT).

• **Protokół** określa protokół ruchu sieciowego. Wybór opcję „Pokaż wszystkie usługi" z rozwijanego menu, wyświetlona zostanie rozszerza lista dostępnych protokołów. Wybierz protokół lub dodaj nowy, korzystając z opcji „Zdefiniowany przez użytkownika". Rozpoczniemy sekwencję, która doda usługę, reprezentującą protokół.

Operacja - definiuje, jakie działania zostaną podjęte odnośnie reguły ALG, wybierając z rozwijanego menu jedną z akcji.

Logowanie, monitor reguły.

• **Loguj pakiety dopasowane do tej reguły**, zaznacz to pole wyboru, aby zalogować pierwszy pakiet z połączenia, które zostało dopasowane do tej reguły.

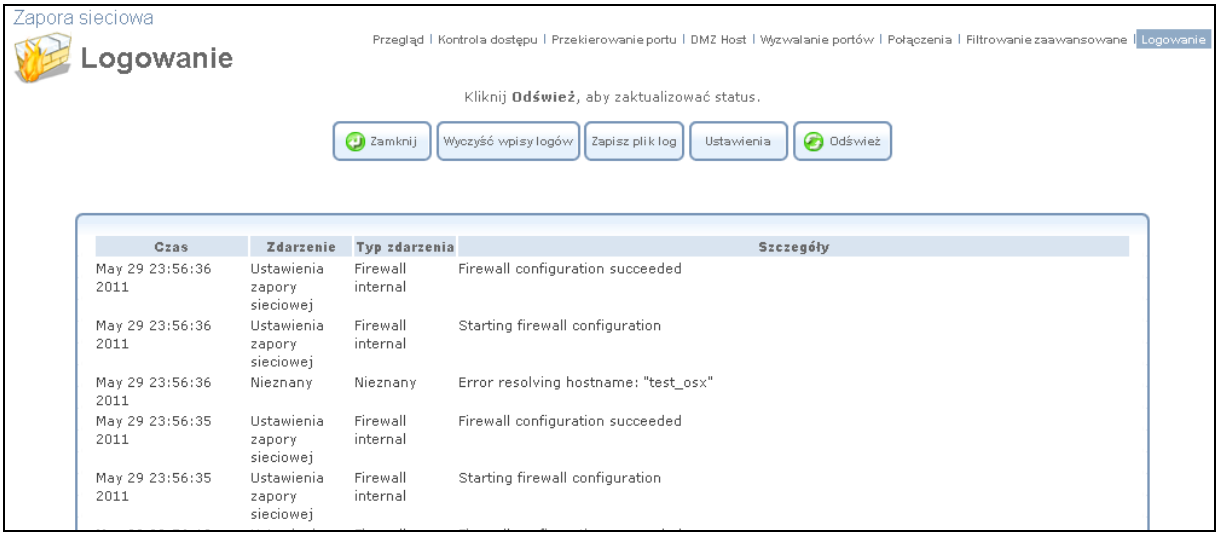
Harmonogram, domyślnie reguła będzie zawsze aktywna. Można jednak określić czas segmentów, w którym reguły mogą być aktywne, wybierając opcję „Definiowane przez użytkownika" z rozwijanego menu. Jeżeli więcej niż jedna reguła jest określona, harmonogram z rozwijanego menu pozwala na możliwość wyboru między dostępnymi regułami. Aby dowiedzieć się, jak skonfigurować harmonogram reguł, odnieś się do „Określenie reguł harmonogramu" w części administracyjnej instrukcji OpenRG.

Uwaga: Zdefiniowane reguły ALG będą miały również zastosowanie do procesów potomnych wniosku, który wykorzystuje wybrany protokół.

Kolejność pojawiania się reguły stanowi zarówno kolejność, w jakiej zostały one określone i sekwencję, w których będą stosowane. Możesz zmienić tę kolejność już po zdefiniowaniu reguł (bez konieczności kasowania, a następnie ponownie je dodać), za pomocą ikon (strzałka - góra, dół)

5.2.8. Przeglądanie dziennika zapory sieciowej

Sekcja „Logowanie" wyświetla listę wydarzeń związanych z zaporą sieciową, w tym próby ustanowienia połączeń przychodzących i wychodzących, próby uwierzytelniania za pośrednictwem interfejsu administracyjnego (WBM lub terminalu telnet), konfiguracje zapory sieciowej i system automatycznego startu.



Rysunek 5.32 Logowanie zdarzeń zapory sieciowej

Dziennik kolumny:

Czas - czas wystąpienia zdarzenia.

Zdarzenie - istnieje pięć rodzajów zdarzeń:

• Ruch przychodzący: zdarzenie jest wynikiem przychodzącego pakietu.

• Ruch wychodzący: zdarzenie jest wynikiem wychodzącego pakietu.

• Ustawienia zapory sieciowej: wiadomość konfiguracyjna.

• Logowanie WBM: wskazuje, że użytkownik zalogował się do WBM.

• Logowanie CLI: Wskazuje, że użytkownik zalogował się do CLI (przez telnet).

Typy zdarzeń - tekstowy opis zdarzenia:

• Zablokowane: pakiet został zablokowany. Wiadomość jest w kolorze czerwonym.

• Akceptowane: pakiet został przyjęty. Wiadomość jest w kolorze zielonym.

Szczegóły - więcej szczegółów na temat pakietu lub zdarzenia, takie jak protokół, adres IP, porty itp.

Przyciski w górnej części strony:

Zamknij - zamknij ekran logowania i powróć do strony głównej OpenRG.

Wyczyść logi - wyczyść rejestr wszystkich aktualnie wyświetlanych wiadomości.

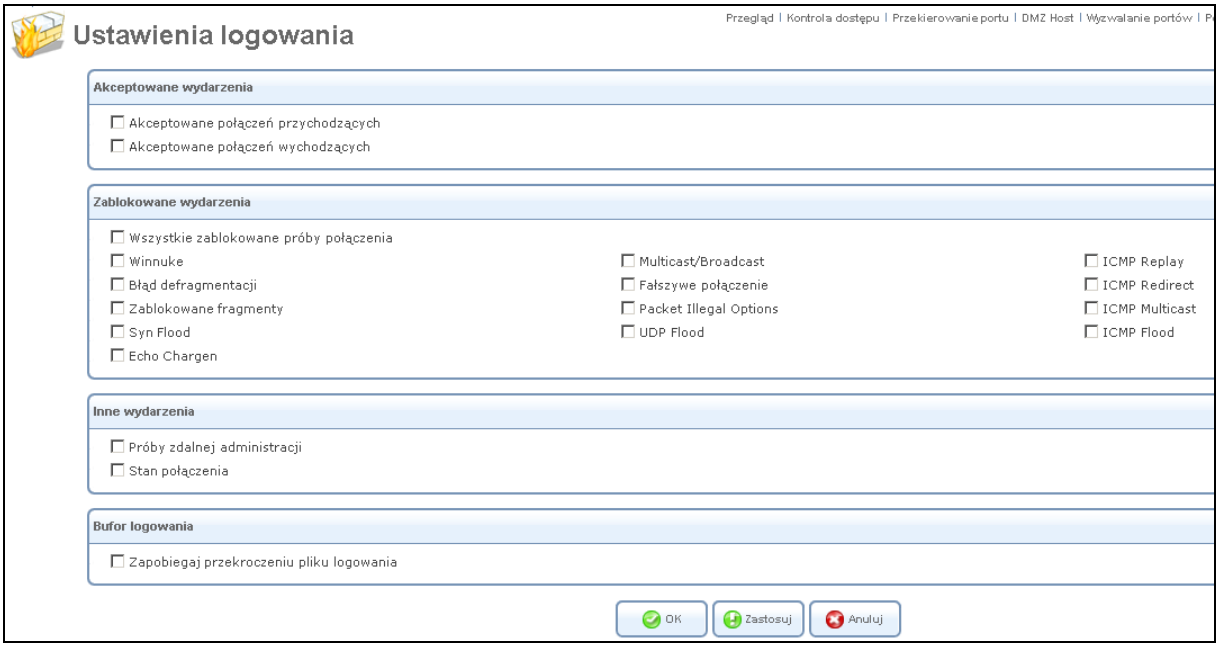
Pobierz plik log – pobierz dziennik jako oddzielony przecinkami plik (CSV), o nazwie firewall.csv.

Ustawienia - przeglądaj lub zmień ustawienia dziennika zabezpieczeń (wyjaśnienie poniżej).

Odśwież - odśwież ekran, aby wyświetlić zachowane najnowsze wiadomości z logów.

Aby wyświetlić lub zmienić ustawienia dziennika zabezpieczeń:

1. Kliknij przycisk „Ustawienia”, który pojawia się u góry ekranu „Zapora sieciowa – Logowanie”. Ustawienia ekranu zostaną wyświetlone.



Rysunek 5.33 Ustawienia logowania

2. Wybierz rodzaje działalności, dla której chcesz mieć generowany komunikat dziennika:

• Akceptowane wydarzenia

Akceptowane połączenia przychodzące - napisz wiadomość dziennika dla każdej udanej próby ustanowienia połączenia przychodzącego z sieci domowej.

Akceptowane połączenia wychodzące - napisz wiadomość dziennika dla każdej udanej próby ustanowienia połączenia wychodzącego do sieci publicznej.

• Zablokowane wydarzenia

Wszystkie zablokowane próby połączenia - napisz wiadomość dziennika dla każdej próby zablokowanego ustanowienia połączenia przychodzącego z sieci domowej lub na odwrotnie. Można włączyć rejestrowanie zablokowanych pakietów określonych rodzajów przez wyłączenie tej opcji, a także zezwolenie niektórych z bardziej szczegółowych opcji poniżej.

Szczególne wydarzenia określa specyficzne zablokowane zdarzenia, które powinny być monitorowane. Przykład takiego wydarzenia, jest SynFlood. Wiadomość o takim zdarzeniu zostanie wygenerowana, jeśli odpowiednie pole wyboru zostanie zaznaczone, lub zaznaczona będzie opcja „Wszystkie zablokowane próby połączenia".

• Inne wydarzenia

Próby zdalnej administracji - napisz wiadomość do dziennika dla każdej próby zdalnej administracji, udanej lub nie.

Status połączenia - podaje dodatkowe informacje o każdej zmianie w połączeniu otwartym przez zaporę sieciową. Ta opcja służy do śledzenia połączeń przez zaporę sieciową i bramę poziomu aplikacji (ALG).

Bufor logowania

Zapobieganie przekroczenia miejsca - zaznacz to pole wyboru, aby zatrzymać rejestrowanie działań na zaporze sieciowej, gdy pamięć przeznaczona na zapisy dziennika zostanie zapełniona.

3. Kliknij przycisk „OK.", aby zapisać ustawienia.

5.2.8.1 Rodzaje zdarzeń zapory sieciowej

Poniżej znajdują się dostępne typy zdarzeń, które mogą być zapisane w logach systemowych:

1. Wewnętrzna zapora sieciowa - objaśnienia z mechanizmu wewnętrznej zapory sieciowej będą dopisywane w przypadku tego typu jako zdarzenie rejestrowane.
2. Zapora sieciowa zmieniła status – zapora sieciowa zmieniła status z góry na dół lub w inny sposób, jak określono w opisie typu zdarzenia.
3. Pakiet STP - pakiet STP został zaakceptowany/odrzucony.

4. Niewłaściwe opcje pakietów - pole opcji w nagłówku pakietu jest albo niewłaściwe, lubzabronione.
5. Rozdrobnienie pakietu - fragment został odrzucony.
6. Ochrona WinNuke - atak WinNuke został zablokowany.
7. Odpowiedź ICMP – wiadomość odpowiedź ICMP została zablokowana.
8. Ochrona przekierowania ICMP - przekierowanie wiadomości ICMP zostało zablokowane.
9. Błędny pakiet w połączeniu - pakiet został zablokowany, będąc na nieprawidłowym połączeniu.
10. Ochrona ICMP - nadawanie komunikatu ICMP zostało zablokowane.
11. Ochrona Broadcast/Multicast – pakiet z broadcast/multicast ze źródłowego adresu IP został zablokowany.
12. Fałszowanie ochrony - pakiet z sieci WAN ze źródłowym adresem IP LAN został zablokowany.
13. Pakiet sieciowy DMZ - pakiet z sieci strefy zdemilitaryzowanej został zablokowany.
14. Zaufane urządzenie - pakiet od zaufanego urządzenia został przyjęty.
15. Polityka domyślna - pakiet został przyjęty/zablokowany zgodnie z polityką domyślną.
16. Zdalna administracja - pakiet przeznaczony do zarządzania OpenRG został przyjęty/zablokowany.
17. Kontrola dostępu - pakiet został przyjęty/zablokowany zgodnie z zasadą kontroli dostępu.
18. Kontrola rodzicielska - pakiet został zablokowany zgodnie z zasadą kontroli rodzicielskiej.
19. Niepowodzenie NAT – niepowodzenie NAT dla tego pakietu.
20. DHCP żądanie - OpenRG skierowała wniosek DHCP (w zależności od dystrybucji).
21. DHCP odpowiedź - OpenRG otrzymał odpowiedź DHCP (w zależności od dystrybucji).
22. Agent przekazywania DHCP - pakiet przekazywania DHCP został odebrany (w zależności od dystrybucji).
23. Pakiet IGMP - pakiet IGMP został zaakceptowany.
24. Połaczenie multicast IGMP – pakiet multicast został zaakceptowany.

25. Pakietu RIP – pakiet RIP został zaakceptowany.
26. Połączenie PPTP - pakiet pyta czy OpenRG jest gotowe do odbioru PPTP. Połączenie zostało zaakceptowane.
27. Zarządzania kluczami kerberos 1293 - związane z bezpieczeństwem, do wykorzystania w przyszłości.
28. Kerberos 88 - do wykorzystania w przyszłości.
29. Żądanie AUTH:113 - pakiet wychodzący na protokołu AUTH został zaakceptowany (dla maksymalnego poziomu bezpieczeństwa).
30. Pakiet-Kabel - do wykorzystania w przyszłości.
31. IPv6 przez IPv4 - IPv6 przez IPv4 pakiet został zaakceptowany.
32. ARP - pakiet ARP został zaakceptowany.
33. Odkryty PPP – odkryty pakiet PPP został zaakceptowany.
34. Sesja PPP - pakiet sesji PPP został zaakceptowany.
35. 802.1Q - 802.1Q (VLAN), pakiet został zaakceptowany.
36. Wychodzący Auth1X - pakiet wychodzący Auth1X został zaakceptowany.
37. IP w wersji 6 - pakiet IPv6 został zaakceptowany.
38. Rozpoczęcie ruchu przez OpenRG - cały ruch, który inicjuje OpenRG jest rejestrowany.
39. Aktywna usługa maksymalnego bezpieczeństwa - pakiet został zaakceptowany, ponieważ należy do dopuszczonej usługi w maksymalnym poziomie bezpieczeństwa.
40. Ochrona SynCookies - pakiet SynCookies został zablokowany.
41. Ochrona ICMP Flood - pakiet został zablokowany, zatrzymano ICMP flood.
42. Ochrona UDP Flood - pakiet został zablokowany, zatrzymano UDP flood.
43. Usługa - pakiet został przyjęty ze względu na pewne usługi, jak określono w przypadku typu.
44. Zaawansowana reguła filtrowania - pakiet został przyjęty/zablokowany ze względu na zaawansowany filtr reguły.
45. Rozdrobnienie pakietu, nagłówek jest za mały - pakiet został zablokowany, ponieważ po defragmentacji, nagłówek jest za mały.
46. Rozdrobnienie pakietu, nagłówek jest zbyt duży - pakiet została zablokowany, ponieważ po defragmentacji, nagłówek jest zbyt duży.

47. Rozdrobnienie pakietu, odrzuć wszystkie bez informacji zwrotnej - nie używane.
48. Rozdrobnienie pakietu, złe wyrównanie - pakiet została zablokowany, ponieważ po defragmentacji, pakiet został źle ustawiony.
49. Rozdrobnienie pakietu, pakiet zbyt duży - pakiet została zablokowany, ponieważ po defragmentacji pakietów był zbyt duży.
50. Rozdrobnienie pakietu, pakiet przekracza wartość - pakiet została zablokowany, ponieważ po defragmentacji znaleziono więcej fragmentów niż jest dozwolone.
51. Rozdrobnienie pakietów, brak pamięci - rozdrobniony pakiet została zablokowany, ponieważ wykryto brak pamięci na fragmenty.
52. Pakiet rozdrobniony, pokrywa się - pakiet została zablokowany, ponieważ po defragmentacji, nie było zachodzących na siebie fragmentów.
53. Niepowodzenie defragmentacji - fragment był przechowywany w pamięci i zablokowany dla wszystkich przybyłych fragmentów i defragmentacja mogła zostać zrealizowana.
54. Połączenie otwarte - zazwyczaj komunikat dotyczący debugowania połączenia.
55. Nieokreślone połączenie otwarte - zazwyczaj komunikat dotyczący debugowania połączenia.
56. Nieokreślone połączenie zależne - zazwyczaj komunikat dotyczący debugowania połączenia.
57. Połączenie zamknięte - zwykle komunikat dotyczący debugowania połączenia.
58. Ochrona Echo/Chargen/Quote/Snork - pakiet został zablokowany, chroni przed Echo/Chargen/Quote/Snork.
59. Pierwszy pakiet w związku nie jest pakietem SYN - pakiet został zablokowany z powodu połączenia TCP, który rozpoczęło się bez pakietu SYN.
60. Błąd: Brak pamięci - komunikat, informujący, że nowe połączenie nie zostało ustalone z powodu braku pamięci.
61. Błędny pakiet: Niepowodzenie - pakiet został zablokowany, ponieważ jest źle sformułowany.
62. Pasywny atak na ftp-server: klient próbował otworzyć porty serwera - pakiet został zablokowany z powodu nieautoryzowanej próby otwarcia portu serwera.

63. Żądanie port FTP do trzeciej części jest zabronione (możliwość ataku odrzuceń) – pakiet został zablokowany z powodu nieuprawnionego żądania dostępu do portu FTP.
64. Zmiana reguł zapory sieciowej - zbiór reguł zapory sieciowej został zmodyfikowany.
65. Uwierzytelnianie użytkowników - wiadomości w czasie logowania, zarówno udanych i nieudanych prób uwierzytelniania.

5.3. Udostępnianie multimediów w sieci domowej

Udostępnianie multimediów za pomocą OpenRG pozwala na współdzielenie i przesyłanie strumieniowe plików multimedialnych z pamięci urządzenia podłączonego do OpenRG. Możesz uzyskać dostęp do udostępnionych plików z sieci albo za pomocą zewnętrznych urządzeń, przykład został opisany w sekcji 5.3.2 lub za pomocą komputera z dostępem do sieci LAN i zainstalowanym na nim oprogramowaniu, jak opisano w punkcie 5.3.3. Obie metody wykorzystują do funkcjonowania Universal Plug and Play (UPnP).

5.3.1. Konfiguracja usługi udostępniania multimediów

Udostępnianie multimediów w OpenRG konfigurujemy, klikając na menu w zakładce „Usługi". Wyświetlony zostanie ekran „Udostępnione multimedia".

Rysunek 5.34 Udostępnione multimedia

Sekcja „Udostępnianie multimedia" zawiera następujące opcje:

Udostępnianie muzyki, zdjęć i filmów w sieci lokalnej. Domyślnie opcja ta jest wybrana. Aby wyłączyć udostępnianie multimediów, odznacz tą opcję i kliknij przycisk „Zastosuj".

Automatycznie udostępnij multimedia we wszystkich folderach. Domyślnie opcja ta jest zaznaczona, powodując automatyczne udostępnienie wszystkich partycji i folderów na podłączeniem urządzeniu zewnętrznym. OpenRG automatycznie przeszukuje podłączone urządzenie pamięci zewnętrznej pod katem plików multimedialnych i wyświetla foldery zawierające takie pliki w sekcji „Foldery lokalne". Aby wyłączyć automatyczne udostępnianie multimediów we wszystkich folderach i ręcznie określić partycje lub foldery zawierające multimedia, wykonaj następujące czynności:

1. Usuń zaznaczenie pola wyboru przy funkcji „Automatycznie udostępnij multimedia we wszystkich folderach" i kliknij przycisk „Zastosuj", następnie odśwież ekran.

Rysunek 5.35 Tryb ręcznego udostępniania multimediów

Status pola zostanie zmieniony na „Brak udziałów", wyświetlona zostanie nowa sekcja, która pozwala na tworzenie i zarządzanie listą ręcznie dodanych wspólnych partycji i folderów.

2. Kliknij link „Dodaj Folder” lub ikonę „Dodaj”. Zostanie wyświetlony ekran „Ustawienia folderu”.

Rysunek 5.36 Ustawienia folderu

3. W polu „Folder” wpisz dokładną ścieżkę (na przykład A/Muzyka, gdzie „A”oznacza partycję, „Muzyka” to folder na tej partycji).

Uwaga: Oznaczenie partycji nie może być zmienione. OpenRG automatycznie przypisuje oznaczenie do partycji, gdy urządzenie magazynujące jest podłączone. Aby uzyskać więcej informacji, zobacz w punkcie 5.4.2.

4. W polu „Tytuł” wpisz nazwę opisująca folder (na przykład, „Muzyka Rock”). Uwaga, wprowadzenie tych informacji jest obowiązkowe.

5. Kliknij przycisk „OK”, aby zapisać ustawienia. Ekran „Udostępnianie multimedia” wyświetla udostępnioną partycję. Jeśli to konieczne, proszę powtórzyć tę samą procedurę, aby dodać kolejne partycje i ich foldery.

W każdej chwili można edytować ustawienia udostępnionych partycji lub folderów, klikając na ikonę działania udziału. Ponadto, możesz usunąć partycję lub folder z listy udziałów, klikając na ikonę „Usuń”.

Uwaga: W przypadku zmiany ustawień udostępniania, kliknij przycisk „Skanuj ponownie" w interfejsie WBM „Udostępnianie multimedia". Wyświetlone zostaną aktualne udziały i dostęp do udostępnionych zdalnie multimediów. Kliknięcie przycisku aktualizacji „Skanuj" spowoduje aktualizację bazy danych mediów z aktualną zawartością wspólnych mediów i ich
ścieżek. Im więcej miejsca na dysku pliki multimedialne zajmują, tym dłużej proces skanowania może potrwać.

OpenRG dodaje plik **MEDIASRV.DB** do wszystkich zapisywalnych partycji, plik identyfikuje urządzenie zewnętrzne. Jest to plik indeksu, określający że serwer multimedialny korzysta z dostępu do plików na tym dysku. Dlatego, nie jest zalecane usuwanie tego pliku.

5.3.2. Strumieniowe przesyłanie multimediów do telewizora za pomocą klienckiego urządzenia multimedialnego

OpenRG umożliwia udostępnianie i przesyłanie strumieniowe plików multimedialnych (muzyka, zdjęcia i video) z podłączonego urządzenia pamięci masowej do telewizora, przez klienta multimediów. W poniższych sekcjach wyjaśniono, jak podłączyć urządzenie do telewizora i bramy, jak również jak udostępnić strumień multimedialny innym użytkownikom.

5.3.2.1. Podłączenie klienta multimediów

Nowoczesne multimedialne urządzenia zawiera klientów zawierają wsparcie dla usługi Universal Plug and Play (UPnP). Zazwyczaj jest to urządzenie posiadające złącze RCA lub koncentryczne dla telewizora, a także posiadają często port LAN i/lub interfejs bezprzewodowy LAN do połączenia z naszą bramą multimediów.

1. Podłącz TV do urządzenia klienta multimediów według instrukcji dostarczonych z urządzenia. Upewnij się, że wybierasz odpowiednie wejście AV na telewizorze.
2. Podłącz multimedialne urządzenie klienckie do wolnego portu Ethernet naszej bramy dostępowej.

Uwaga: Jeśli urządzenie klienta multimedialnego korzysta z sieci bezprzewodowej, może połączyć się z OpenRG bez użycia kabli. Ponieważ jednak korzystanie z przesyłania strumienia multimediów wymaga połączenia wysokiej wydajności, zalecane jest korzystanie z tej funkcjonalności tylko wtedy, gdy klient/klienci - urządzenia multimedialne obsługują protokół 802.11n.

5.3.2.2. Przeglądanie plików i mediów strumieniowych

Odbiór multimedialnej transmisji serwera OpenRG przez multimedialne urządzenie klienckie jest automatyczny, nie wymaga żadnej dodatkowej konfiguracji.

1. Włącz multimedialne urządzenie klienckie. Poniższe zdjęcia przedstawiają przykładowe urządzenie klienckie z wyświetlonym na telewizorze menu (podane przykładowe urządzenie klienckie jest podłączone do OpenRG).

Rysunek 5.37 Główny ekran przykładowego urządzenia klienckiego

2. Do obsługi urządzenia klienckiego używamy pilota zdalnego sterowania, aby wybrać „Moje multimedia". Ścieżka dostępu do danych OpenRG zostanie wyświetlona (zawiera nazwę dysku).

Rysunek 5.38 Wyświetlony udział na naszym OpenRG

3. Wybierz udział OpenRG, wyświetlona zostanie lista dostępnych danych.

Rysunek 5.39 Zawartość udostępnionego folderu OpenRG

Uwaga: Multimedialne urządzenie klienckie wyświetla taką samą hierarchię katalogów, jak na podłączonym do OpenRG urządzeniu pamięci zewnętrznej.

4. Wybierz folder, na przykład „Zdjęcia". Zawartość folderu zostanie wyświetlana na ekranie.

Rysunek 5.40 Wyświetlona zawartość udostępnionego katalogu

6. Wybierz przykładowy plik do wyświetlenia

Rysunek 5.41 Wyświetlona fotografia

Z tej samej metody skorzystamy, aby strumieniowo przesyłać muzykę i pliki wideo z dysku do telewizora.

5.3.3. Dostęp do udostępnionych danych z komputera w sieci LAN

W tej sekcji dowiemy się, jak uzyskać dostęp do treści multimedialnych z dowolnego komputera będącego w sieci lokalnej, na którym zainstalowana została aplikacja kliencka (UPnP). Jednym z takich zastosowań jest projekt **XBMC Media Center**. Poniższy przykład wykorzystuje XBMC do przedstawienia, jak uzyskać dostęp do plików multimedialnych za pomocą komputera w sieci LAN. Po zainstalowaniu tej aplikacji na komputerze, wykonaj następujące czynności:

1. Uruchom XBMC. Wyświetlony zostanie główny ekran.

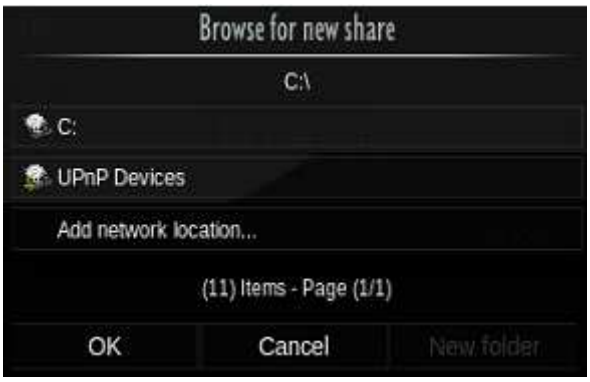
Rysunek 5.42 Główny ekran XBMC

2. Wybierz typ nośnika, który chcieliby Państwo zobaczyć klikając na odpowiedni link (filmy, muzyka lub obrazki). Na przykład wybieramy opcję „Muzyka". Pojawi się następujący ekran.

Rysunek 5.43 Dodawanie źródła

3. Aby uzyskać dostęp do pożądanych plików multimedialnych, należy najpierw zdefiniować ścieżkę do udostępnionego katalogu, w którym są przechowywane pliki multimedialne. Aby to zrobić, wykonaj następujące czynności:

a. Wybierz „Dodaj źródło" (patrz rysunek 5.43) i kliknij przycisk „Przeglądaj" w następnym oknie. Wyświetlone zostanie ekran „Przeglądaj w poszukiwaniu nowych udziałów".



Rysunek 5.44 Przeglądaj w poszukiwaniu nowych udziałów

b. Wybierz opcję „Urządzenie UPnP". Zostanie wyświetlone nowe okno dialogowe.

Rysunek 5.45 Link z danymi multimedialnymi OpenRG

Link „Jungo Media Server" zapewnia dostęp do urządzeń zewnętrznych podłączonych do OpenRG.

c. Kliknij ten link. Po przeskanowaniu urządzenie do przechowywania treści multimedialnych, XBMC wyświetla wspólne partycje, na których zostały wykryte pliki.

Rysunek 5.46 Wspólna partycja zawierająca pliki multimedialne

d. Kliknij na link do współdzielonej partycji, aby pliki z katalogami multimedialnymi zostały wyświetlone.

Rysunek 5.47 Udostępnione multimedialne katalogi

Należy pamiętać, że XBMC wyświetla tą samą hierarchię katalogów, co na urządzeniu pamięci zewnętrznej.

e. Wybierz katalog, w którym żądane pliki multimedialne się znajdują.

f. Aby zapisać ścieżkę do katalogu z multimediami, kliknij „OK", w katalogu kliknij „Przeglądaj" w poszukiwaniu nowych udziałów. Wyświetlone zostanie nowe okno dialogowe. Spowoduje to utworzenie skrótu o nazwie „Jungo Media Server" do wybranego katalogu, co pozwala na dostęp do plików multimedialnych z XBMC.

Rysunek 5.48 Skrót „Jungo Media Server"

4. Kliknij skrót „Jungo Media Server". Lista plików multimedialnych zapisanych w wybranym katalogu zostanie wyświetlana.

Rysunek 5.49 Pliki multimedialne w udostępnionym katalogu

Uwaga: W przypadku katalogu multimediów określonego w ścieżce, zawierającego podkatalogi, zostanie wyświetlony po kliknięciu na link „Jungo Media Server". Wybierz żądany katalog, aby wyświetlić pliki w nim zawarte.

5. Kliknij na link pliku, aby rozpocząć jego odtwarzanie z XBMC.

Podobnie, należy wykonać powyższą procedurę w celu określenia ścieżki do innych plików multimedialnych, do których będziemy chcieli uzyskać dostęp.

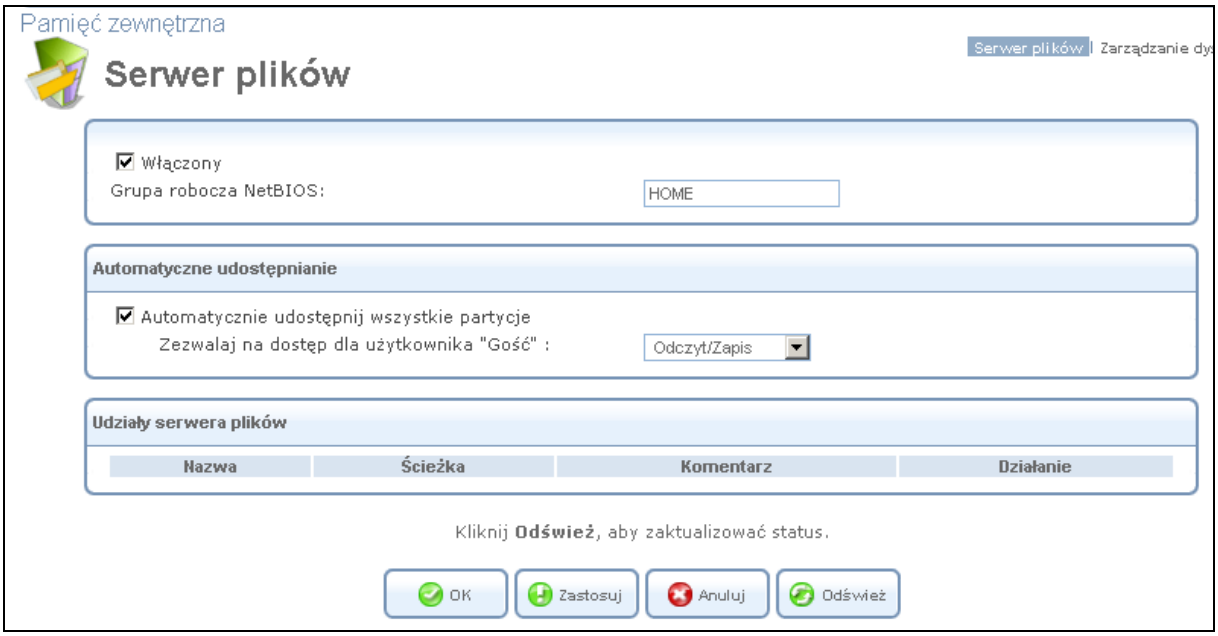
5.4. Zarządzanie udostępnionymi zasobami

OpenRG może działać jako menedżer dysków podłączonych poprzez USB. W sieci domowej możemy wykorzystać podłączone zewnętrzne pamięci jako zmapowany dysk sieciowy, a także wymieniać informacje bez bezpośredniego dostępu do siebie.

5.4.1. Zarządzanie serwerem plików

OpenRG zawiera narzędzie serwera plików, który pozwala na wykonywanie różnych zadań na plikach, np. jak zarządzać udziałami serwera plików i zdefiniować listę kontroli dostępu. Gdy urządzenie pamięci zewnętrznej jest podłączone do OpenRG, wszystkie partycje dysku są automatycznie udostępniane domyślnie.

Dostęp do ustawień serwera plików uzyskamy klikając na pozycję „Pamięć zewnętrzna" w menu zakładki „Usługi". Wyświetlony zostanie ekran „Serwer plików".



Rysunek 5.50 Serwer plików

Włączony - zaznacz lub odznacz pole wyboru, aby włączyć lub wyłączyć tą funkcję.

Grupa robocza NetBIOS - nazwa grupy roboczej, która będzie wyświetlana w systemie otoczenia sieciowego w naszej sieci lokalnej. Wszystkie komputery podłączone do sieci OpenRG będą widoczne w tej grupie roboczej.

Automatyczne udostępnianie wszystkich partycji - partycje urządzenia zewnętrznego podłączonego do OpenRG są automatycznie wyświetlane i udostępnianie wszystkim komputerom w sieci LAN. Funkcja ta jest domyślnie włączona.

Zezwalaj na dostęp dla gości – z rozwijanego menu, możemy wybrać poziom uprawnień, zgodnie z nadanymi uprawnieniami dla użytkowników sieci LAN dostęp do udziału może być realizowany:

Oczyt/Zapis - każdy użytkownik sieci może odczytywać i zapisywać w udostępnionych katalogach bez konieczności uwierzytelniania.

Tylko do odczytu - każdy użytkownik sieci może tylko odczytywać udostępnione pliki.

Wyłączony - użytkownicy sieci LAN muszą uwierzytelniać się, aby uzyskać dostęp do udziału. Będą mieć możliwość korzystania z udziałów zgodnie z uprawnieniami określonymi przez OpenRG w sekcji „Ustawienia użytkownika".

Udziały serwera plików - wszystkie partycje są wyświetlane automatycznie i udostępniane. Sekcja ta pozwala na przeglądanie udziałów i plików na partycji.

5.4.1.1 Korzystanie z serwera plików w systemie Mac

W celu podłączenia do serwera plików OpenRG z komputera Mac, wykonaj następujące czynności:

1. Na komputerze Mac podłączonym do OpenRG, kliknij przycisk „Połącz z serwerem" z menu „Go". Wyświetlony zostanie ekran „Połącz z serwerem".

Rysunek 5.51 Połącz z serwerem

2. W polu adres serwera, wpisz smb://192.168.1.254, a następnie kliknij przycisk „Połącz". Pojawi się nowe okno, wyświetlające dostępne udziały plików.

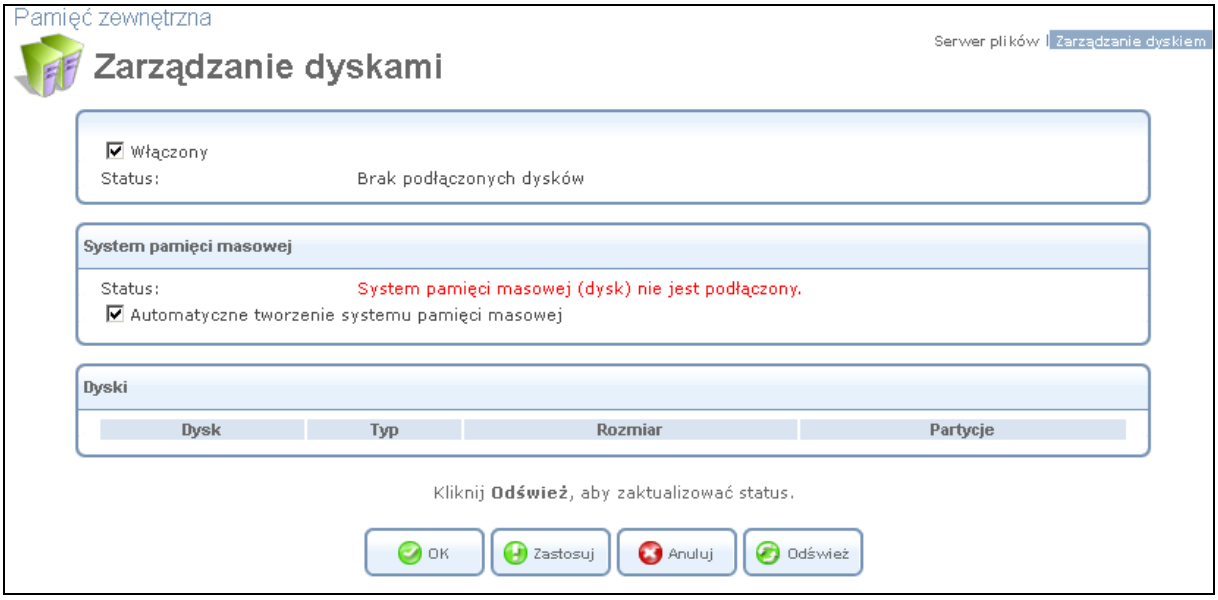
Rysunek 5.52 Połączenie z serwerem

3. Wybierz udział, do którego chcesz się połączyć. Jeśli pojawi się monit, wprowadź poprawną nazwę użytkownika i hasło. Następnie kliknij przycisk „OK.". Po nawiązaniu połączenia pojawi się zawartość udziału.

Rysunek 5.53 Udział serwera

5.4.2. Zarządzanie dyskami

Sekcja menu „Pamięć zewnętrzna" umożliwia dostęp do ekranu „Zarządzanie dyskami", który pozwala na przeglądanie i zarządzania urządzeniami pamięci masowej.

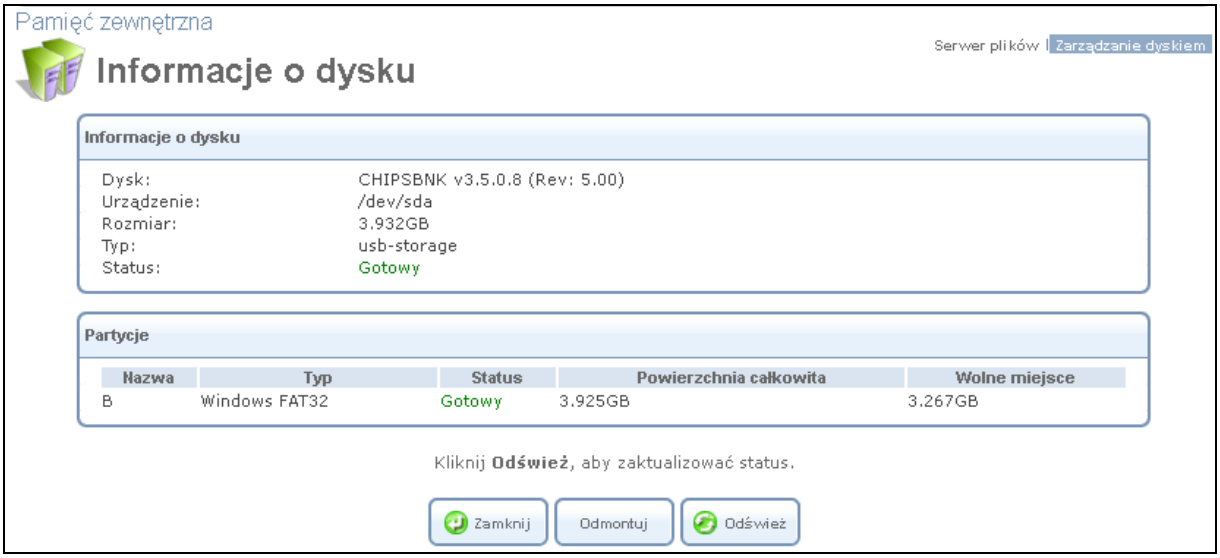


Rysunek 5.54 Zarządzanie dyskami

Włączony - zaznacz lub odznacz pole wyboru, aby włączyć lub wyłączyć tą funkcję.

System pamięci zewnętrznej OpenRG - automatycznie określa miejsce na urządzeniu do przechowywania danych używanych przez różne usługi. To ustawienie jest poprawne dla odłączonych urządzeń pamięci zewnętrznej. Po ponownym podłączeniu, OpenRG może wybrać inną partycję dla tego celu.

Dyski - ta sekcja zawiera szczegółowe informacje na temat podłączonych urządzeń pamięci masowej. Kliknij nazwę dysku. Wyświetlony zostanie ekran „Informacje o dysku" – wyświetla wszelkie dostępnych informacje dotyczące dysku i jego partycji.



Rysunek 5.55 Informacje o dysku

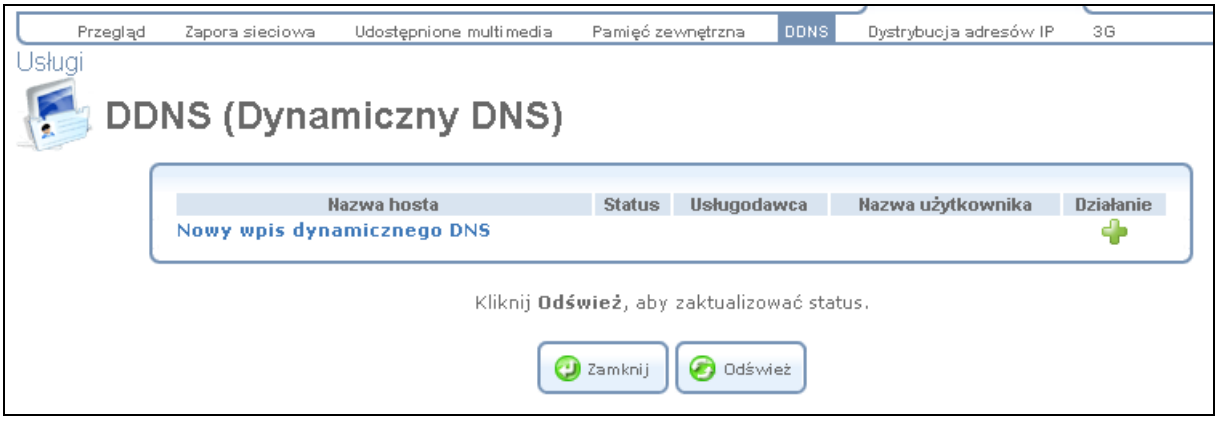
5.5. Dostęp do sieci za pomocą nazwy domeny

Usługa OpenRG „Dynamiczny DNS" (DDNS) pozwala zdefiniować unikalną nazwę domeny dla bramy połączenia internetowego, co pozwala na dostęp do OpenRG lub usług w sieci domowej, po prostu wpisując w przeglądarce internetowej nazwę tej domeny. Gdy korzystamy z tej funkcji, nie trzeba będzie sprawdzać i zapamiętywać adresu zewnętrznego IP bramy, który może ulec zmianie w przypadku odłączenia od sieci dostawcy usług internetowych lub zmiana może być wymuszona po stronie dostawcy.

5.5.1. Otwarcie konta usługi „Dynamiczny DNS"

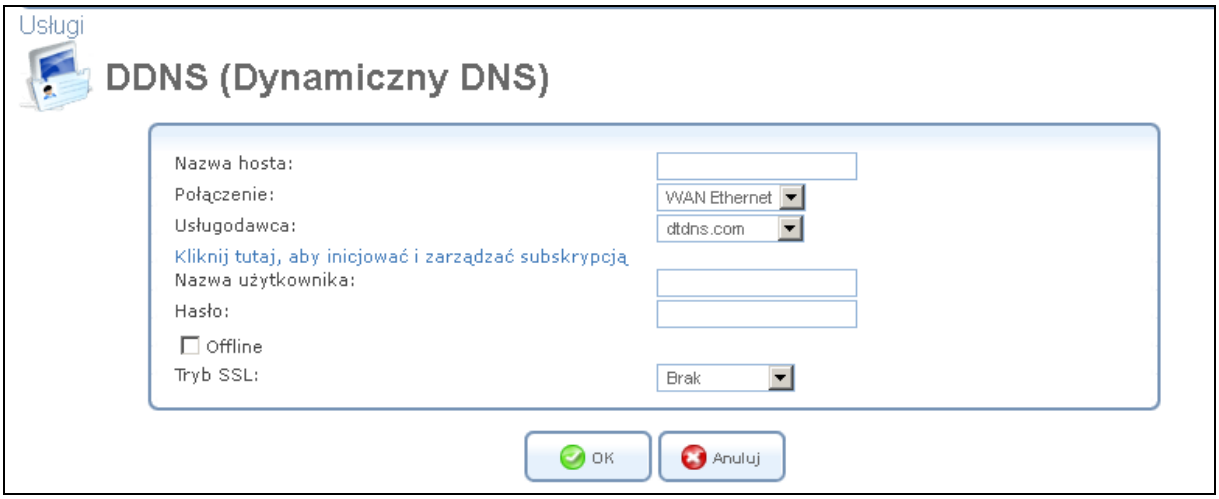
W celu korzystania z funkcji DDNS, należy najpierw się zarejestrować, usługi serwera DDNS są świadczone, np. za darmo przez kilka firm (np. dyndns.org). OpenRG zawiera listę popularnych serwerów DDNS, na których możemy utworzyć takie darmowe konto. Aby wyświetlić listę wykonaj następujące czynności:

1. W zakładce „Usługi” należy kliknąć na pozycję menu „DDNS”. Wyświetlony zostanie ekran usługi dynamicznego serwera nazw domenowych.



Rysunek 5.56 Dynamiczny DNS

2. Kliknij na link „Nowy wpis dynamicznego DNS”, aby dodać nowy wpis DDNS. Wyświetlony zostanie ekran, jak poniżej.



Rysunek 5.57 Nowy wpis DDNS

3. Określ parametry konta DDNS

Nazwa hosta - wpisz swoją pełną nazwę domeny DDNS (np. xxxxxx@dyndns.info).

Dostawca - wybierz dostawcę usługi DDNS. Na ekranie lista zostanie odświeżona, wyświetlając parametry wymagane przez danego operatora. Dostawca - opisany w tym dokumencie jest dyndns.org, dostarczy nam wszystkie potrzebne parametry, które otrzymamy po założeniu konta u danego dostawcy usług.

Kliknij tutaj, aby inicjować i zarządzać subskrypcją - kliknij ten link, a otworzona zostanie strona www wybranego dostawcy tworzenia konta dla usługi DDNS. Na przykład, gdy wybieramy dyndns.org po kliknięciu na link wyświetlona zostanie strona, strona: http://www.dyndns.com/account/.

Nazwa użytkownika - wprowadź nazwę użytkownika DDNS (nazwa, którą należy podać to zwykle nazwa loginu do naszego operatora usługi DDNS).

Hasło - podaj hasło DDNS (hasło, które należy podać to zwykle hasło logowania do naszego operatora usługi DDNS).

Wildcard – wybierz to pole, aby umożliwić stosowanie linków, takich jak np. http://www.<your host>.dyndns.com.

Wymiana poczty - wpisz swój adres serwera wymiany poczty, aby przekierować wszystkie wiadomości e-mail na Twój adres DDNS do serwera poczty.

Kopia zapasowa MX - zaznaczenie tego pola wyboru, aby wyznaczyć zapasowy serwer wymiany poczty.

Offline - jeśli chcemy, aby czasowo nasza witryna była w trybie offline (zapobiega dotarciu ruchu do naszej nazwy domeny DDNS), zaznacz to pole wyboru, aby włączyć przekierowanie zapytań DNS do alternatywnego adresu URL, definiowanych na koncie DDNS. Dostępność tej funkcji zależy od poziomu naszego konta i rodzaju usług, jakie posiadamy.

Tryb SSL - wersje OpenRG posiadają wsparcie dla „Secure Socket Layer" (SSL), zabezpieczone usługi DDNS są dostępne przy użyciu protokołu HTTPS. Po podłączeniu, OpenRG sprawdza certyfikat serwera DDNS. Użyj tej pozycji, aby wybrać metodę sprawdzania poprawności certyfikatu.

Brak - nie weryfikować certyfikatu serwera.

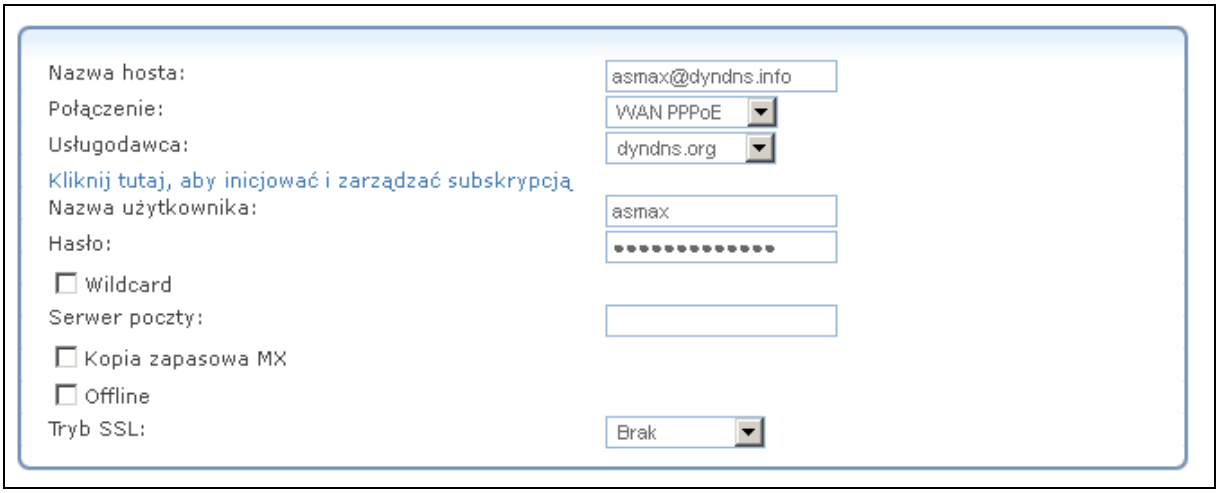
Łańcuch - sprawdź cały łańcuch certyfikatów. Po wybraniu tej opcji na ekran zostanie odświeżony (patrz rysunek 5.58), wyświetlając dodatkowe rozwijane menu, aby zweryfikować ważność certyfikatu. Wybierz odpowiednio opcję „Ignoruj" lub „Sprawdź". Jeśli certyfikat utracił ważność, połączenie zostanie natychmiast rozłączone.

Rysunek 5.58 Tryb SSL

Skieruj - upewnij się, że certyfikat serwera jest bezpośrednio podpisany przez główny certyfikat. Opcja ta zapewnia również opcję menu „Zatwierdzanie czasu", określającą zakres zatwierdzania ważności certyfikatu, jak opisano powyżej.

Uwaga: Jeśli posiadamy, na przykład założone darmowe konto w serwisie dyndns.org, wtedy potrzebujemy tylko login, hasło i dodać wpis naszego nowego hosta DDNS, czyli nazwę naszej domeny. Po otrzymaniu linku aktywacyjnego na podany email i zalogowaniu się do naszego konta, aby dodać wpis nowego hosta DDNS kliknij na link po lewej stronie My Account → My Services → w głównym oknie widzimy Host Services → klikamy Add hostname → w polu Hostname wpisujemy naszą unikalną nazwę domeny i wybieramy z rozwijanego menu rozszerzenie domeny (proste nazwy mogą już być zajęte) → w polu IP Address klikamy na link Your current location's IP …. → następnie na przycisk niżej Add To

Cart → kolejno Proceed to checkout → Activate Services i po tym kroku posiadamy już nasz własny aktywny wpis DDNS (naszą nazwę hosta DDNS). Przykładowy ekran, jak powinniśmy nasze uzyskane dane wpisać wygląda, jak poniżej.



Rysunek przedstawia przykładowy wpis DDNS, gdzie nazwa hosta podana na rysunku i nazwa użytkownika jest przykładem.

5.6. Konfiguracja dystrybucji adresów IP (DHCP)

Sekcja menu „Dystrybucja adresów IP" funkcja pozwala na łatwe dodawanie komputerów do

sieci domowej. Zapewnia mechanizm przydzielania adresów IP i innych wymaganych parametrów konfiguracyjnych sieci dla komputerów. Funkcja ta jest również znana jako „Serwer DHCP". Serwer DHCP OpenRG dla połączeń przewodowych i bezprzewodowych pracuje na interfejsie LAN Bridge (moście sieciowym LAN).

Host może wybrać, czy wznowić wygasłą dzierżawę lub pozwolić jej wygasnąć. Jeśli zdecyduje się przedłużyć dzierżawę to będzie również otrzymywał aktualne informacje na temat aktywnych usług sieciowych, z poprzedniej dzierżawy mogą już być niedostępne, host pozwala, aby zaktualizowano jego konfiguracji sieci odnośnie ewentualnych zmian, które mogły mieć miejsce od momentu pierwszego podłączenia do sieci. Jeżeli host zakończy dzierżawę przed jej upływem, może wysłać wiadomość opuszczenia dzierżawy do serwera DHCP, który następnie zwolni adres IP jako dostępny do wykorzystania przez innych.

Serwer DHCP naszego urządzenia:

• Wyświetla listę wszystkich urządzeń podłączonych do DHCP OpenRG

• Określa zakres adresów IP, które mogą być przydzielone w sieci LAN

• Definiuje czas, przez który dynamiczne adresy IP są przydzielane

• Zapewnia parametry konfiguracji dla poszczególnych urządzeń sieci LAN i może być skonfigurowany jako włączony/wyłączony oddzielnie dla każdego urządzenia LAN

• Pozwala na przypisanie statycznego IP do komputera LAN, tak, że komputer otrzyma ten sam adres IP za każdym razem, gdy łączy się z naszą siecią, nawet jeśli adres IP jest w zakresie adresów, które serwer DHCP może przydzielić innym komputerom.

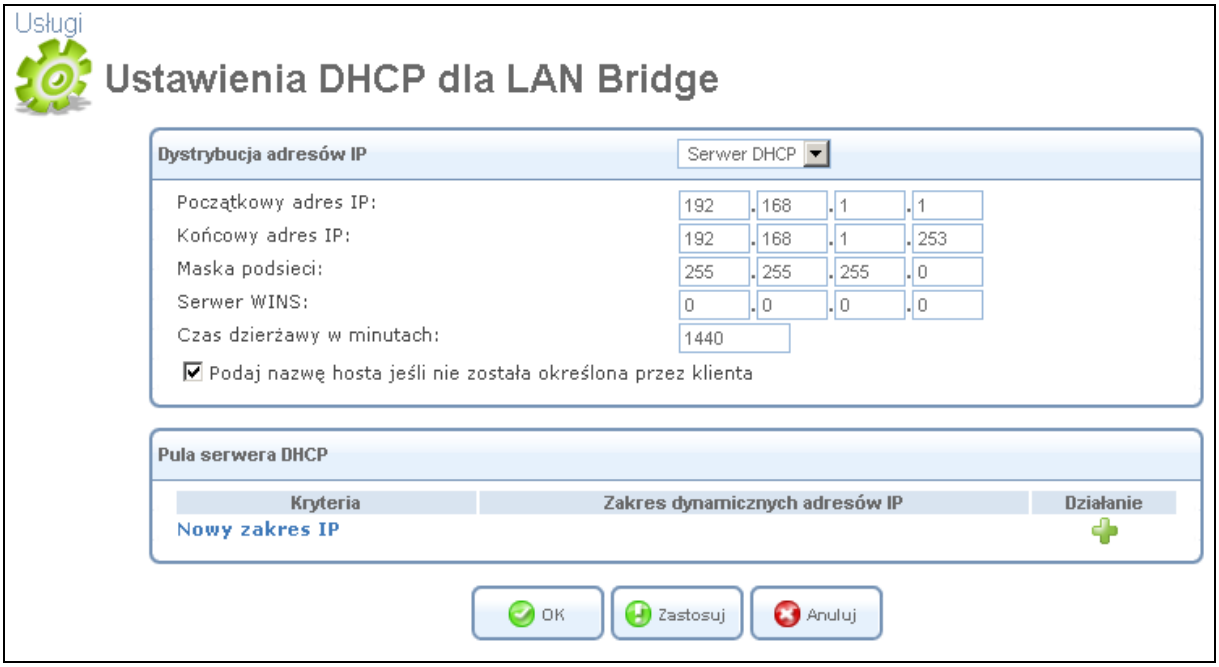
5.6.1. Przeglądanie i konfigurowanie ustawień DHCP

Aby wyświetlić ustawienia serwera DHCP, kliknij przycisk „Dystrybucja adresów IP" w menu zakładki „Usługi". Wyświetlony zostanie ekran „Dystrybucja adresów IP".

Rysunek 5.59 Dystrybucja adresów IP

Aby zmienić ustawienia serwera DHCP dla urządzeń:

1. Kliknij na ikonę „Edytuj" w sekcji „Działanie". Wyświetlony zostanie ekran DHCP.



Rysunek 5.60 Ustawienia serwera DHCP dla LAN Bridge

2. Wybierz usługę DHCP:

Wyłączony - wyłączyć serwer DHCP dla tego urządzenia.

Serwer DHCP - włącz serwer DHCP dla tego urządzenia.

3. W przypadku wybranego serwera DHCP, należy wypełnić następujące pola:

Początkowy adres IP - pierwszy adresu IP, który może być przydzielony do komputera LAN. Domyślny adres IP interfejsu LAN to 192.168.1.254, zaleca się, żeby pierwszy adres IP przypisany do hosta sieci LAN zaczynał się od 192.168.1.2 lub wyżej.

Końcowy adres IP - ostatni adres IP z zakresu, który może być użyty do automatycznego przypisywania parametrów dla komputerów w sieci lokalnej. Domyślnie jest to 192.168.1.253.

Maska podsieci - służy do określenia, w jakim segmencie sieci należy szukać adresu IP. Przykładowa wartość domyślna dla podsieci LAN to 255.255.255.0.

Serwer WINS - jeśli chcesz korzystać z zewnętrznego serwera WINS, należy wpisać jego adres IP i kliknąć „OK”.

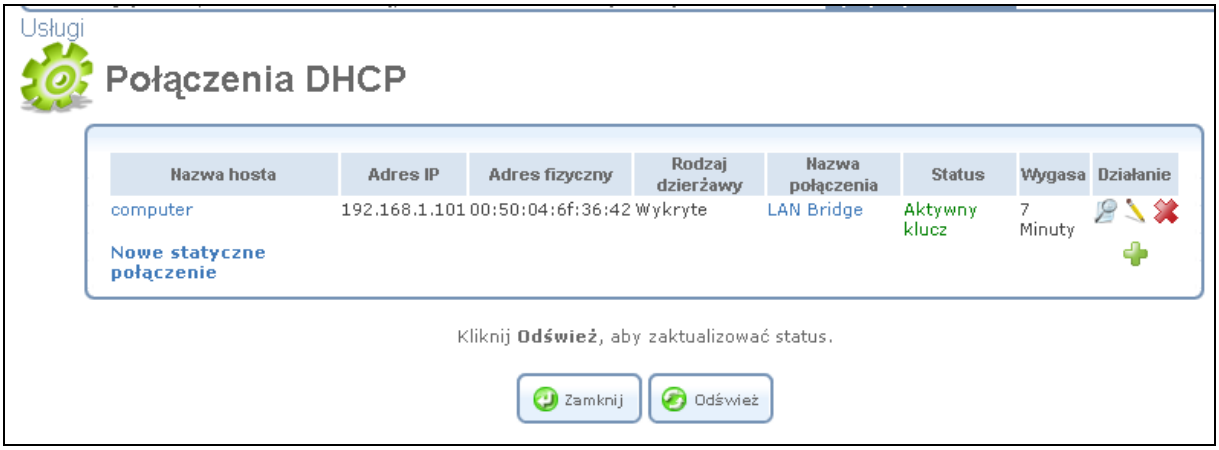
Czas dzierżawy w minutach - każde urządzenie będzie otrzymywać przypisany adres IP przez serwer DHCP do czasu połączenia z siecią. Po wygaśnięciu dzierżawy serwer będzie ustalał, czy komputer jest odłączony od sieci. Jeśli tak, serwer może przypisać adres IP do nowo podłączonego komputera. Funkcja ta zapewnia, że adresy IP, które nie są w użyciu będą dostępne dla innych komputerów w sieci.

Podaj nazwę hosta jeśli nie została określona przez klienta - jeśli klient DHCP nie ma nazwy hosta, brama będzie automatycznie przypisywać taką nazwę dla niego.

4. Kliknij przycisk „OK”, aby zapisać ustawienia.

5.6.2. Połączenia DHCP

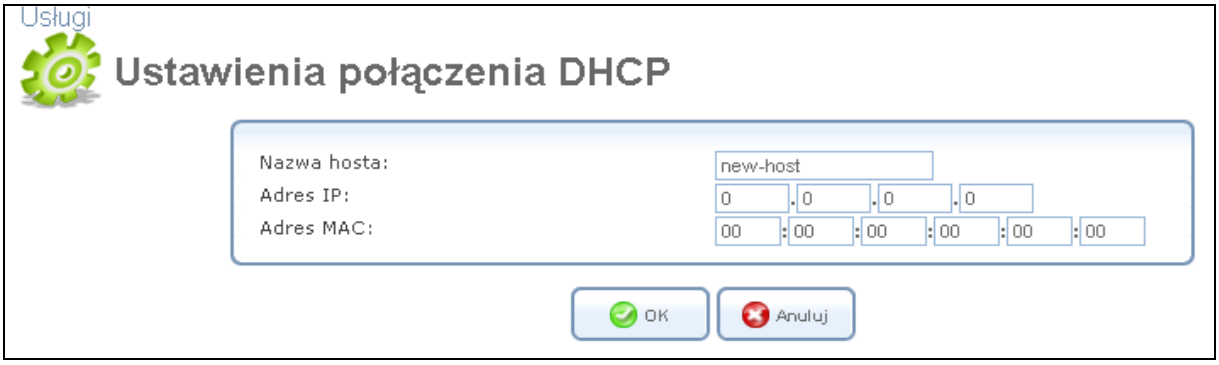
Aby wyświetlić listę komputerów obecnie korzystających z serwera DHCP, kliknij „Lista połączeń”. Wyświetlony zostanie ekran „Połączenia DHCP”.



Rysunek 5.61 Połączenia DHCP

Aby zdefiniować nowe połączenie ze stałym adresem IP:

1. Kliknij przycisk „Nowe statyczne połączenie”. Wyświetlony zostanie ekran „Ustawienia połączenia DHCP”.



Rysunek 5.62 ustawienia połączenia DHCP

2. Wprowadź nazwę hosta dla tego połączenia.

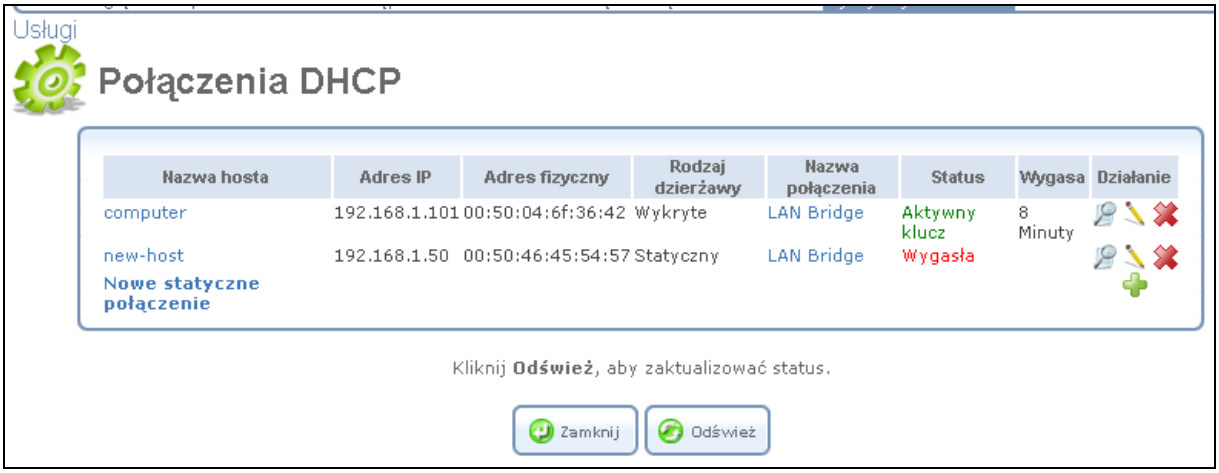
3. Wpisz stały adres IP, który chcesz mieć przypisany do komputera.

4. Wpisz adres MAC karty sieciowej komputera.

Uwaga: Stały adres IP jest aktualnie przypisany do konkretnej karty sieciowej (NIC) zainstalowanej w komputerze LAN, a dokładnie do jej adresu MAC. Jeśli wymienimy kartę sieciową, należy zaktualizować wpis na liście połączeń DHCP i podać nowy adres MAC karty sieciowej.

5. Kliknij przycisk „OK”, aby zapisać wprowadzone ustawienia.

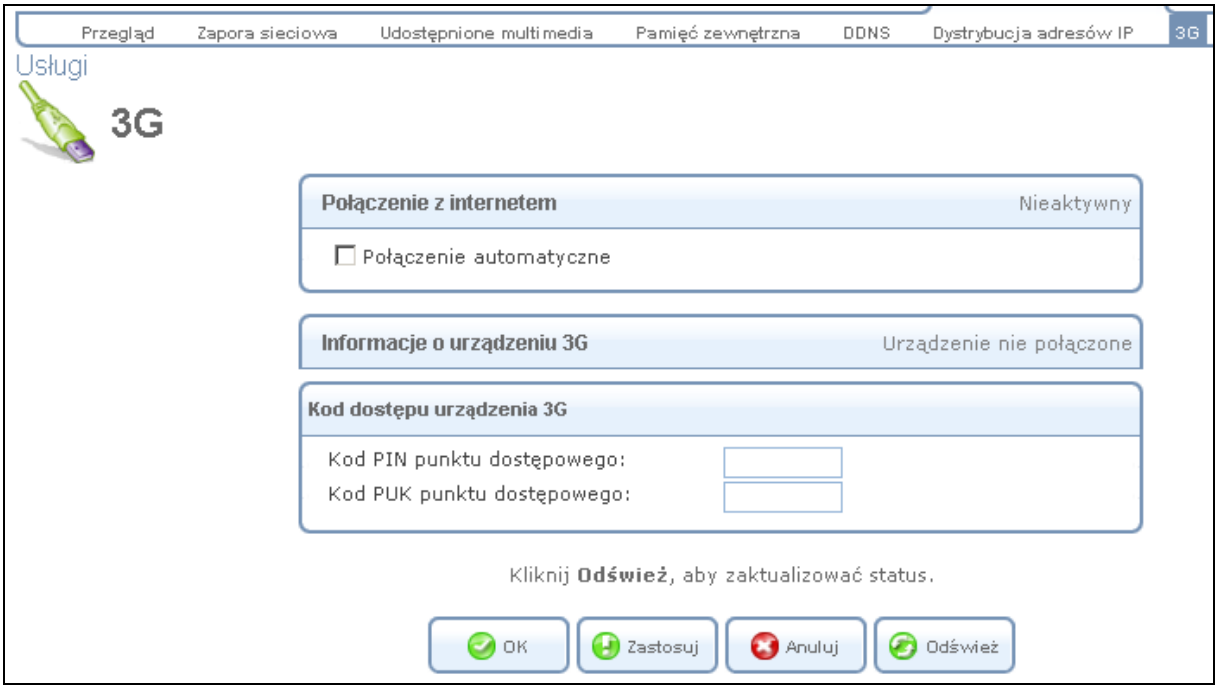
Sekcja „Połączenia DHCP” pojawi się ponownie (patrz rysunek 5.63), wyświetlone zostaną określone statyczne połączenia. To połączenie może być edytowane lub usuwane przy użyciu standardowych ikon działania.



Rysunek 5.63 Połączenie DHCP

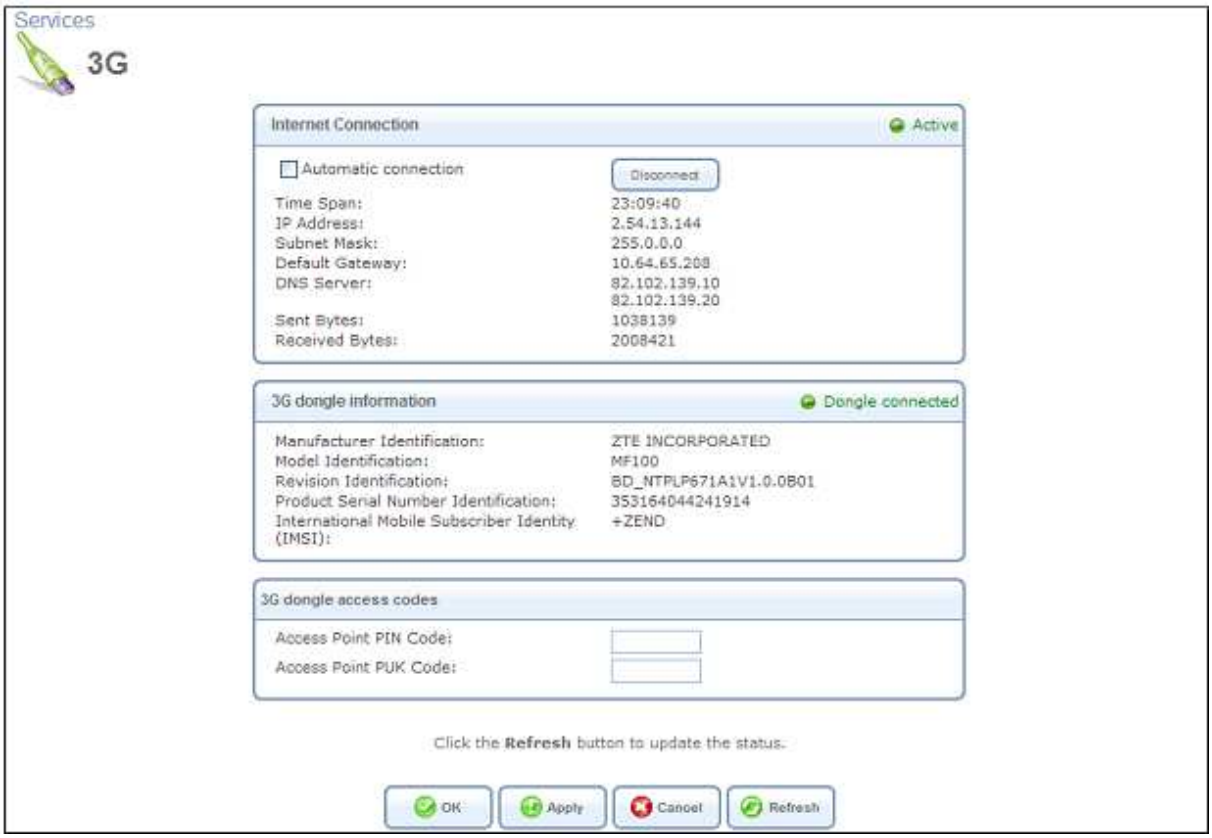
5.7. Łączenie się z internetem 3G

Oprócz możliwości użycia jako połączenia WAN łącza DSL lub Ethernet, nasze urządzenie OpenRG posiada jeszcze jedną możliwość połączenia WAN, a jest to funkcja połączenia komórkowego 3G. To połączenie służy jako połączenie rezerwowe, gdyby nasze standardowe połączenie z WAN, np. przez ADSL z jakiegokolwiek powodu przestało działać. Podłącz do portu USB OpenRG modem 3G. Modem 3G musi być wcześniej aktywowany i posiadać aktywne konto u operatora. Następnie kliknij pozycję zakładki „3G" w menu „Usługi". Wyświetlony zostanie ekran „3G".



Rysunek 5.64 3G

Aby połączyć się z Internetem za pomocą połączenia komórkowego 3G, kliknij „Połącz". W sekcji „Połączenie z Internetem" i prawej części okna.



Rysunek 5.65 Połączenie 3G

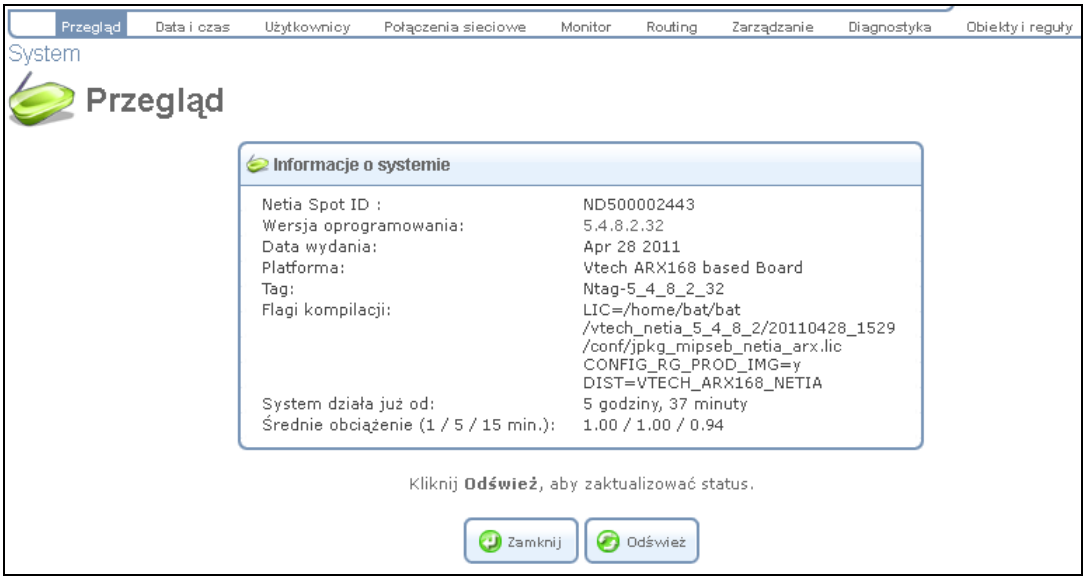
Można zakończyć połączenie w dowolnej chwili, klikając przycisk „Rozłącz" lub zaznaczyć pole wyboru „Automatyczne połączenie" (i kliknij przycisk „Zastosuj"), jeśli chcesz, aby połączenie 3G łączyło się automatycznie jako pierwsze połączenie, gdy główne połączenie (DSL lub Ethernet) zawiedzie i automatycznie rozłączyło połączenie 3G po przywróceniu właściwego połączenia.

Sekcja ta zapewnia również wyczerpujące informacje na temat połączenia i samego podłączonego urządzenia/modemu 3G. Dolna część zawiera pola tekstowe do wprowadzenia kodu PIN i PUK punktu dostępowego. W przypadku, gdy nasz modem 3G jest z jakiegoś powodu został zablokowany. Sieć komórkowa powinna udostępnić te kody w takim przypadku.

6. System

6.1. Przeglądanie informacji o systemie

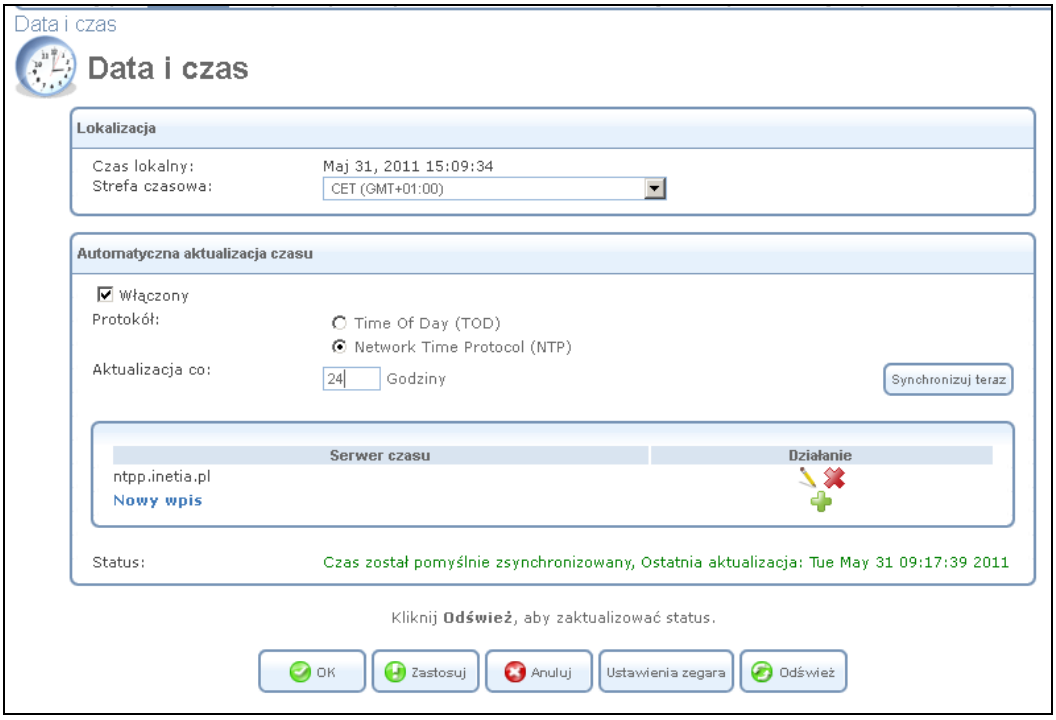
W sekcji „Przegląd" (patrz Rysunek 6.1) wyświetla wersję oprogramowania i sprzętu, jak również jego czasu pracy.



Rysunek 6.1 Przegląd informacji o systemie

6.2. Ustawianie daty i czasu

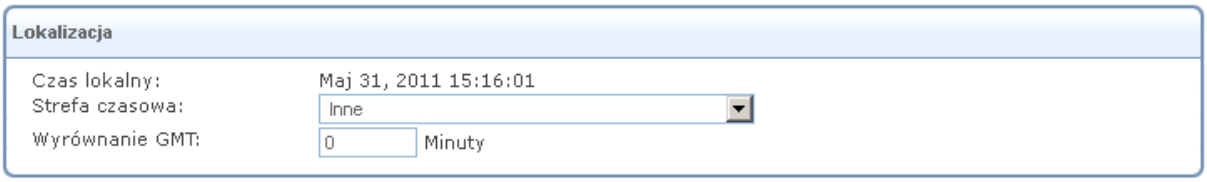
Sekcja „Data i godzina” w menu umożliwia skonfigurowanie bramy i strefy czasowej.



Rysunek 6.2 Ustawienia daty i czasu

• Ustawianie lokalnej strefy czasowej

Z rozwijanego menu wybieramy strefa czasową, która odpowiada aktualnej lokalizacji. Jeśli chcesz, aby ręcznie określić ustawienia strefy czasowej, wybierz opcję „Inne”. Po odświeżeniu ekranu, wyświetlając pole „Wyrównanie GMT”.

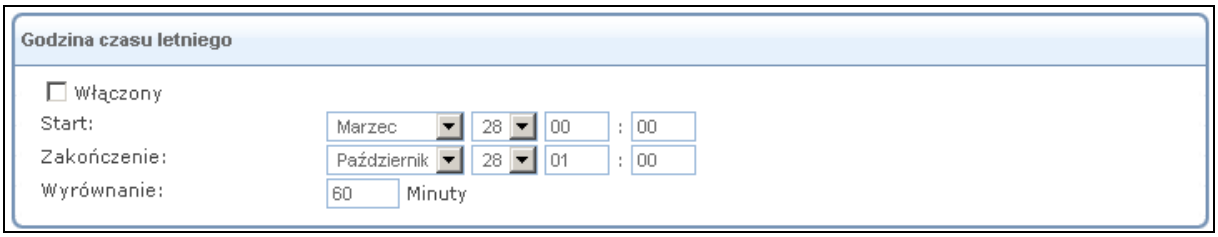


Rysunek 6.3 Lokalna strefa czasowa – Wyrównanie GMT

To pole pozwala na ręczne ustawienie czasu lokalnego z przesunięciem „Greenwich Mean Time” (GMT).

• Konfigurowanie godziny czasu letniego

OpenRG automatycznie wykrywa ustawienia dużej liczby stref czasowych, za pomocą swojej wewnętrznej bazy danych stref czasowych. Istnieje jednak kilka stref czasowych, dla których ustawienia czasu letniego nie zostały ustawione w OpenRG, ponieważ mogą one różnić się od czasu rzeczywistego. W przypadku ustawień letniej strefy czasowej może się ona okresowo zmieniać. W sekcji znajdują się następujące pola, które pozwalają na ręczną konfigurację lokalnego czasu letniego.



Rysunek 6.4 Ustawienia czasu letniego

Włączone - zaznacz to pole wyboru, aby automatycznie włączyć tryb czasu letniego w niżej wymienionych okresach.

Start - data i czas strefy czasowej na czas letni zaczyna się od podanego okresu.

Zakończenia - data i czas strefy czasowej, kończy się od podanego okresu.

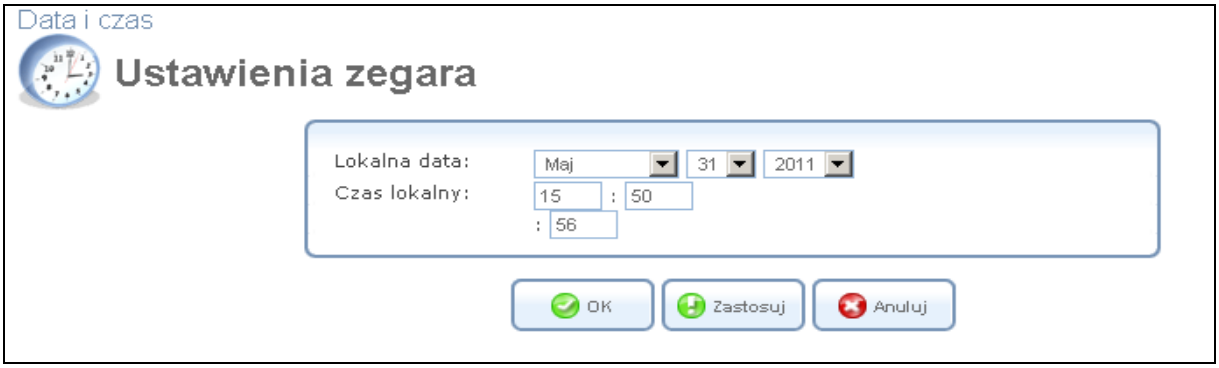
Przesunięcie czasu letniego - przesunięcie od standardowego czasu (zimą).

- Jeśli chcesz przystosować urządzenie do okresowego wykonywania automatycznej aktualizacji czasu, wykonaj następujące czynności (funkcja domyślnie aktywna):

1. Wybierz pole wyboru „Włączone" w sekcji „Automatyczna aktualizacja czasu".
2. Wybierz protokół używany, aby wykonać aktualizację czasu, wybierając „Time of Day" (TOD) lub „Network Time Protocol" (NTP).
3. W polu „Aktualizacja", określamy częstotliwość wykonywania aktualizacji.
4. Domyślnie OpenRG jest skonfigurowany z aktywnym serwerem NTP Netia. Można określić inny adres serwera NTP, klikając link „Nowy wpis" na dole sekcji „Automatyczna aktualizacja czasu". Możesz znaleźć listę serwerów czasu posortowanych według regionów pod adresem: http://www.pool.ntp.org.

Jeśli chcesz ręcznie ustawić czas lokalny i aktualną datę, wykonaj następujące czynności:

1. Kliknij przycisk „Ustawienia zegara”. Wyświetlony zostanie ekran „Ustawienia zegara”.



Rysunek 6.5 Ustawienia zegara

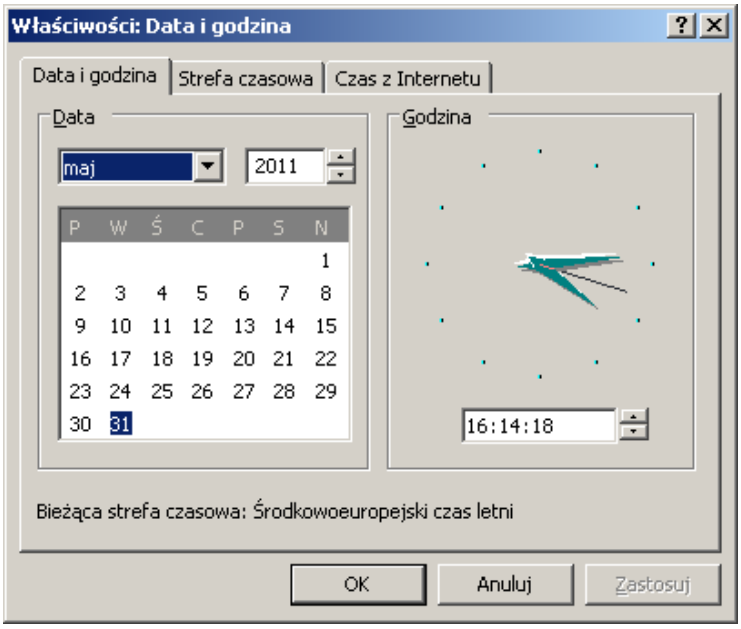
2. Dostosuj ustawienia w razie konieczności i kliknij „OK”. Zostaniesz przekierowany z powrotem do sekcji „Data i czas”.

Ponadto OpenRG może funkcjonować jako serwer „Simple Network Time Protocol” (SNTP), co pozwala na automatyczną aktualizację ustawień czasu na komputerach z jednego, ale wiarygodnego źródła. Domyślnie, opcja serwera SNTP w OpenRG jest włączona. Aby zsynchronizować czas serwera SNTP i komputera PC podłączonego do bramy, wykonaj następujące czynności:

1. W sekcji „Automatyczna aktualizacja czasu” z menu „Data i godzina”, wybierz opcję „Network Time Protocol (NTP)”.
2. Kliknij przycisk „OK”, aby zapisać ustawienia.
3. Na komputerze podłączonym do bramy, wykonaj następujące czynności:

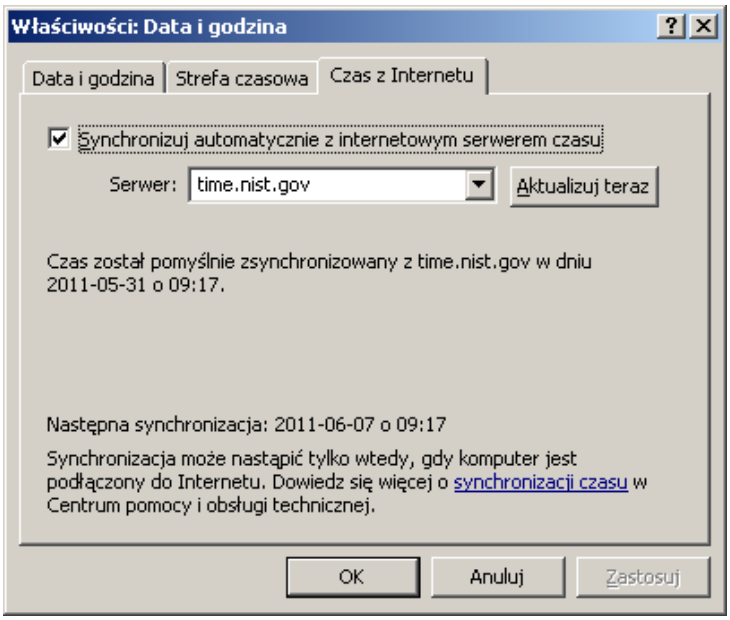
Uwaga: Poniższe wyjaśnienia są oparte na interfejsie użytkownika systemu Windows XP.

1. W Panelu sterowania dwukrotnie kliknij na zakładkę „Data i godzina” (zegarek na pasku zadań). Wyświetlone zostaną okna właściwości.



Rysunek 6.6 Windows - właściwości daty i godziny

2. Kliknij „Czas z Internetu". Wyświetlony zostanie następujący ekran.



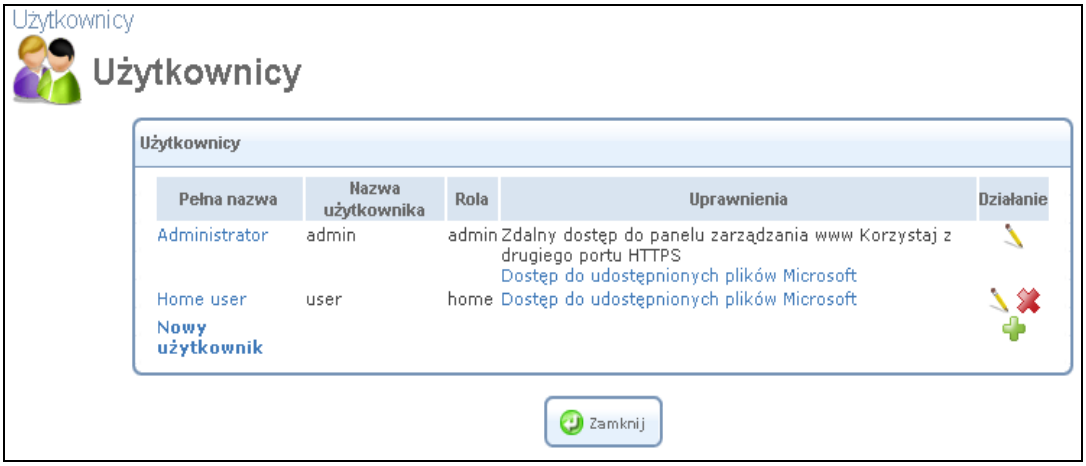
Rysunek 6.7 Windows – Czas z Internetu

3. W polu „Serwer" wprowadź adres IP OpenRG w sieci LAN (domyślnie jest to 192.168.1.254).
4. Kliknij przycisk „Aktualizuj". Windows będzie synchronizowany z serwerem SNTP OpenRG. Ponadto system Windows przeprowadza okresowe synchronizacje z serwerem SNTP.

5. Kliknij przycisk „OK”, aby zapisać ustawienia.

6.3. Zarządzanie użytkownikami

Pozycja menu „Użytkownicy” pozwala na przeglądanie i edytowanie określonych kont użytkowników, jak również tworzyć nowe.

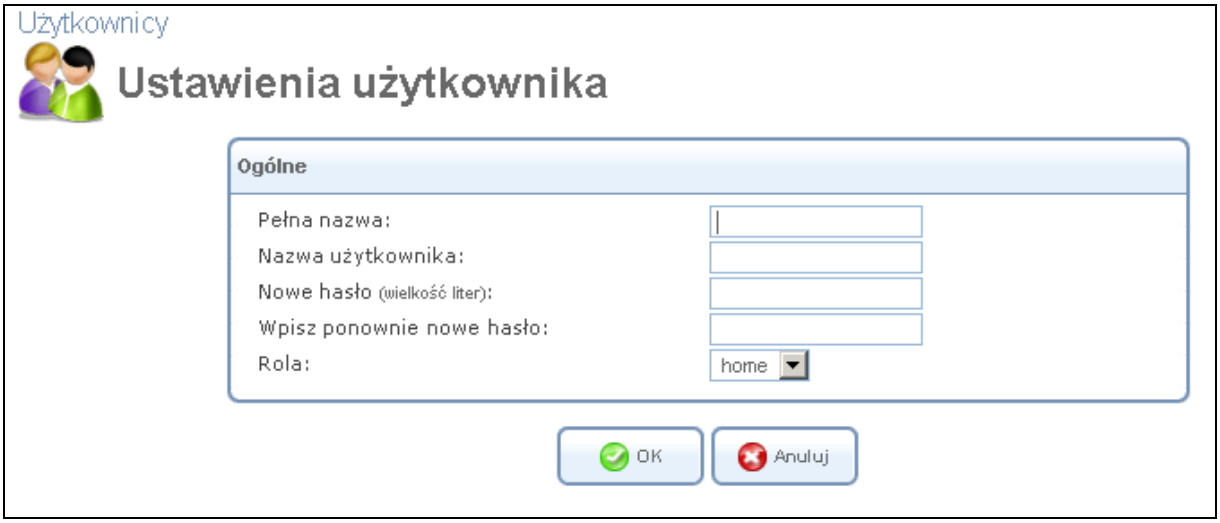


Rysunek 6.8 Użytkownicy

Domyślnie skonfigurowany jest użytkownik „Administrator” i „Home user”. Choć oba konta są edytowalne, administrator nie może zostać usunięty. Można tworzyć dodatkowych użytkowników, jak opisano w następnym rozdziale.

6.3.1. Dodawanie użytkownika

Aby dodać nowego użytkownika, należy kliknąć link „Nowy użytkownik”. Wyświetlony zostanie ekran „Ustawienia użytkownika”.



Rysunek 6.9 Ustawienia użytkownika

Wprowadź następujące informacje:

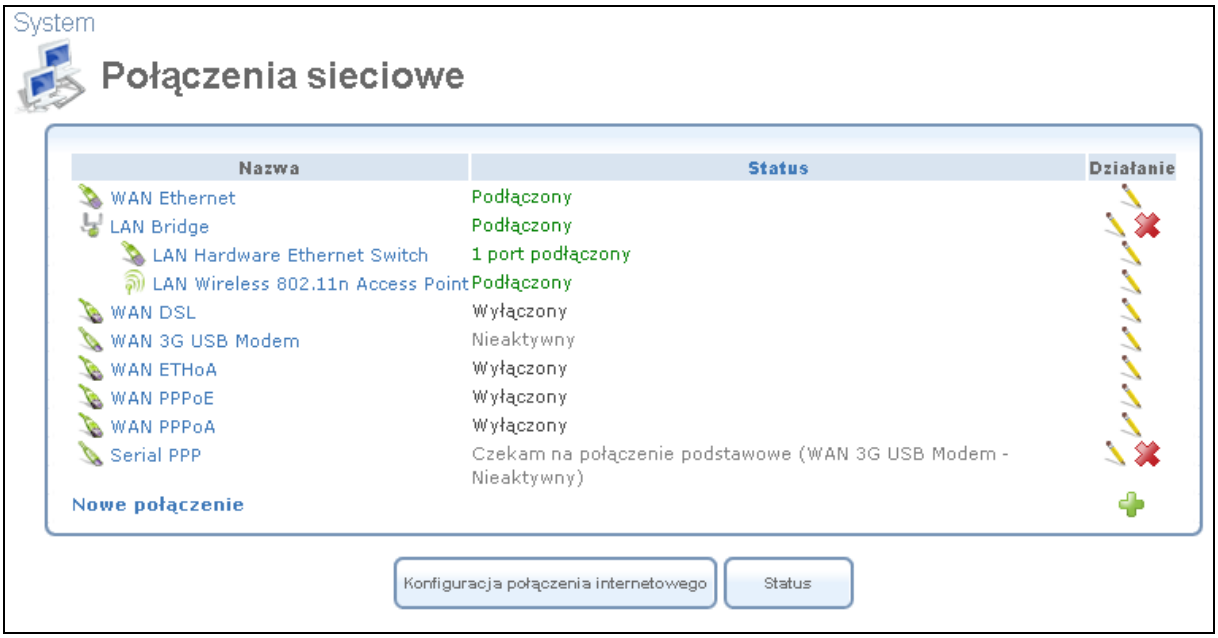
- **Imię i nazwisko** – wprowadź dane użytkownika; imię i nazwisko.
- **Nazwa użytkownika** - nazwa uwierzytelniania, który użytkownik będzie musiał wprowadzić w celu uzyskania dostępu do sieci.
- **Nowe hasło** - hasło użytkownika.
- **Wpisz ponownie nowe hasło** - wpisz hasło ponownie w celu sprawdzenia jego poprawności.
- **Rola** – To rozwijane menu umożliwia zdefiniowanie roli użytkownika, który reprezentuje określony zestaw uprawnień, dostępnych w OpenRG. To ustawienie zezwoleń określa, które funkcje użytkownik będzie mógł używać domyślnie i w jakim zakresie.

Jako administrator, możesz przypisać rolę „home" lub „admin" do nowego użytkownika konta. Rola „home" daje użytkownikowi ograniczony dostęp do WBM.

6.4. Połączenia sieciowe

Ten rozdział opisuje różne połączenia sieciowe dostępne z OpenRG, jak również typy połączeń, które można tworzyć. OpenRG obsługuje zarówno fizyczne i logiczne połączenia sieciowe. Po kliknięciu „Połączenia sieciowe" w menu „System". Ekran „Połączenia

sieciowe" pozwala na konfigurowanie różnych parametrów fizycznego połączenia (LAN i WAN) oraz tworzyć nowe połączenia.



Rysunek 6.10 Połączenia sieciowe

Dostępne są następujące fizyczne typy połączeń OpenRG:

• **LAN** – Tworzenie sieci domowej

LAN Hardware Ethernet Switch (patrz punkt 6.4.3)

LAN Wireless 802.11n Access Point (patrz punkt 6.4.5)

• **WAN** – Połączenie z Internetem

WAN Ethernet (patrz punkt 6.4.6)

WAN DSL (patrz punkt 6.4.7)

WAN 3G USB Modem (patrz punkt 6.4.8)

Logiczne połączenia sieciowe dostępne z OpenRG:

Point-to-Point Protocol przez Ethernet (patrz punkt 6.4.10)

Point-to-Point Protocol przez ATM (patrz punkt 6.4.11)

Ethernet przez ATM (patrz punkt 6.4.12)

LAN Bridge (patrz punkt 6.4.4)

Serial PPP (patrz punkt 6.4.15)

6.4.1. Typy sieci

Każde połączenie sieciowe w OpenRG może być skonfigurowane do pracy w jednym z trzech trybów: WAN, LAN lub DMZ. Zapewnia to dużą elastyczność i większą funkcjonalność. Na przykład, można określić, że połączenie Ethernet LAN na OpenRG będzie działać jako sieć WAN. Oznacza to, że wszystkie hosty w sieci lokalnej będą widziane jako komputery WAN, zarówno przez komputery poza OpenRG i przez OpenRG. WAN i reguły zapory sieciowej mogą być stosowane także w każdej innej sieci WAN.

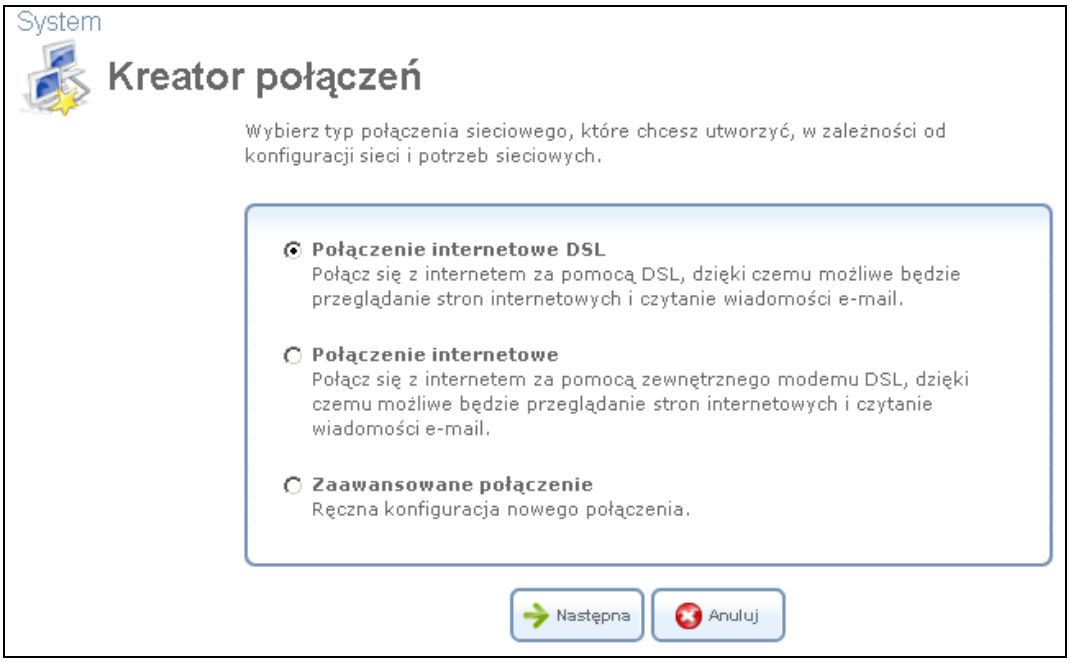
Innym przykładem jest połączenie sieciowe, które określa się jako sieć DMZ (Strefa zdemilitaryzowana). Mimo, że ta sieć jest fizycznie wewnątrz OpenRG, będzie ona działać jako niezabezpieczona, niezależna sieć dla których OpenRG działa tylko jako router.

6.4.2. Połączenie za pomocą kreatora

Logiczne połączenie sieciowe można łatwo utworzyć za pomocą kreatora połączenia. Kreator połączenia składa się z serii kroków, intuicyjnego zarządzania, skonstruowany jest, aby zebrać wszystkie informacje niezbędne do utworzenia połączenia logicznego.

6.4.2.1. Tworzenie połączeń jako brama Ethernet

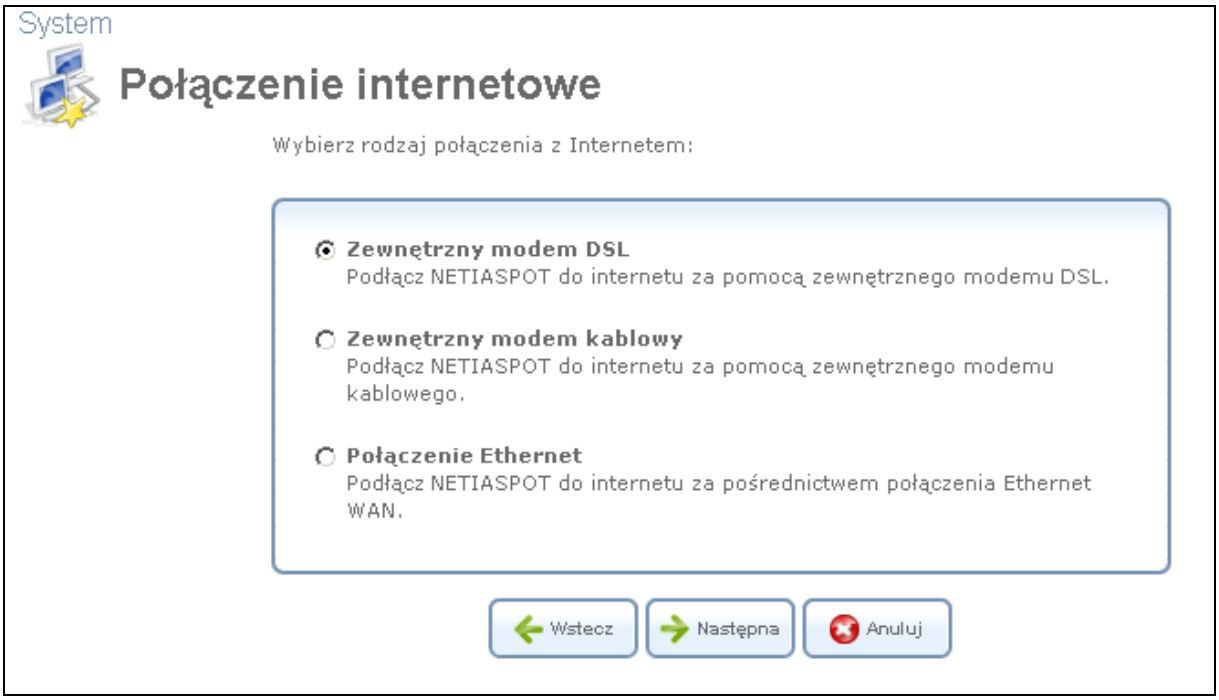
Aby zainicjować konfigurację połączenia za pomocą kreatora, kliknij przycisk „Nowe połączenie", w menu „Połączenia sieciowe". Wyświetlony zostanie ekran „Kreator połączeń".



Rysunek 6.11 Kreator połączeń

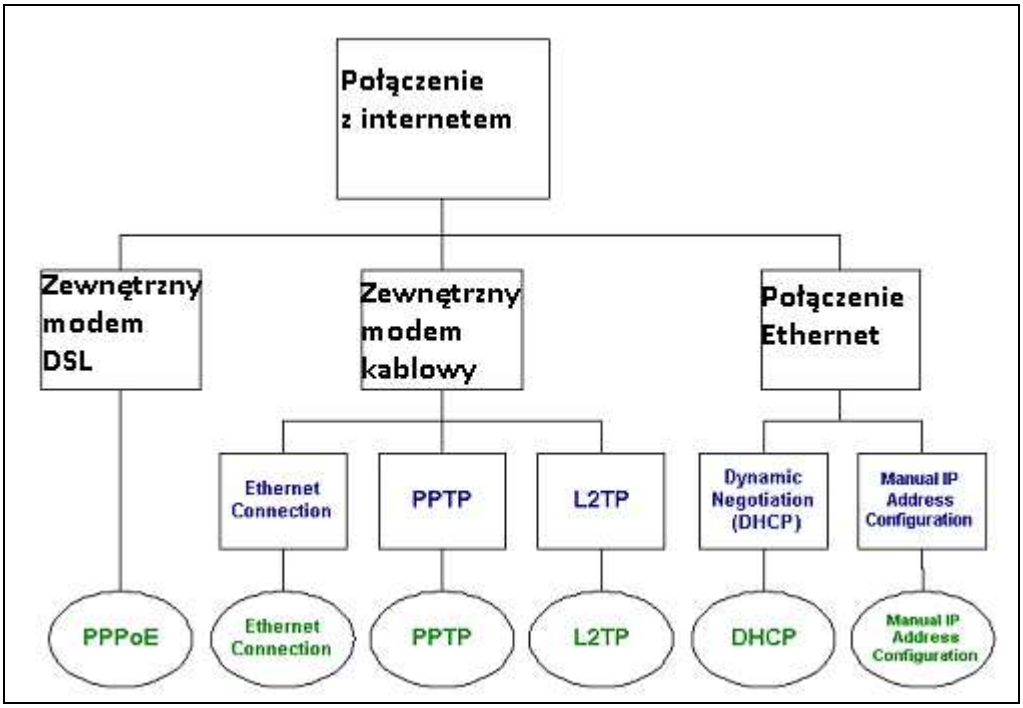
Sekcja ta przedstawia Państwu główne typy połączeń. Każda opcja i jej wybór prowadzi do dodatkowych opcji, dodając więcej informacji przy każdym kroku i zawężając parametry w kierunku uzyskania pożądanego połączenia sieciowego.

• Połączenie internetowe DSL - Wybranie tej opcji powoduje przejście do sekcji „Połączenie internetowe DSL", co pozwala skonfigurować połączenie z internetu, w jednej z dostępnych metod.



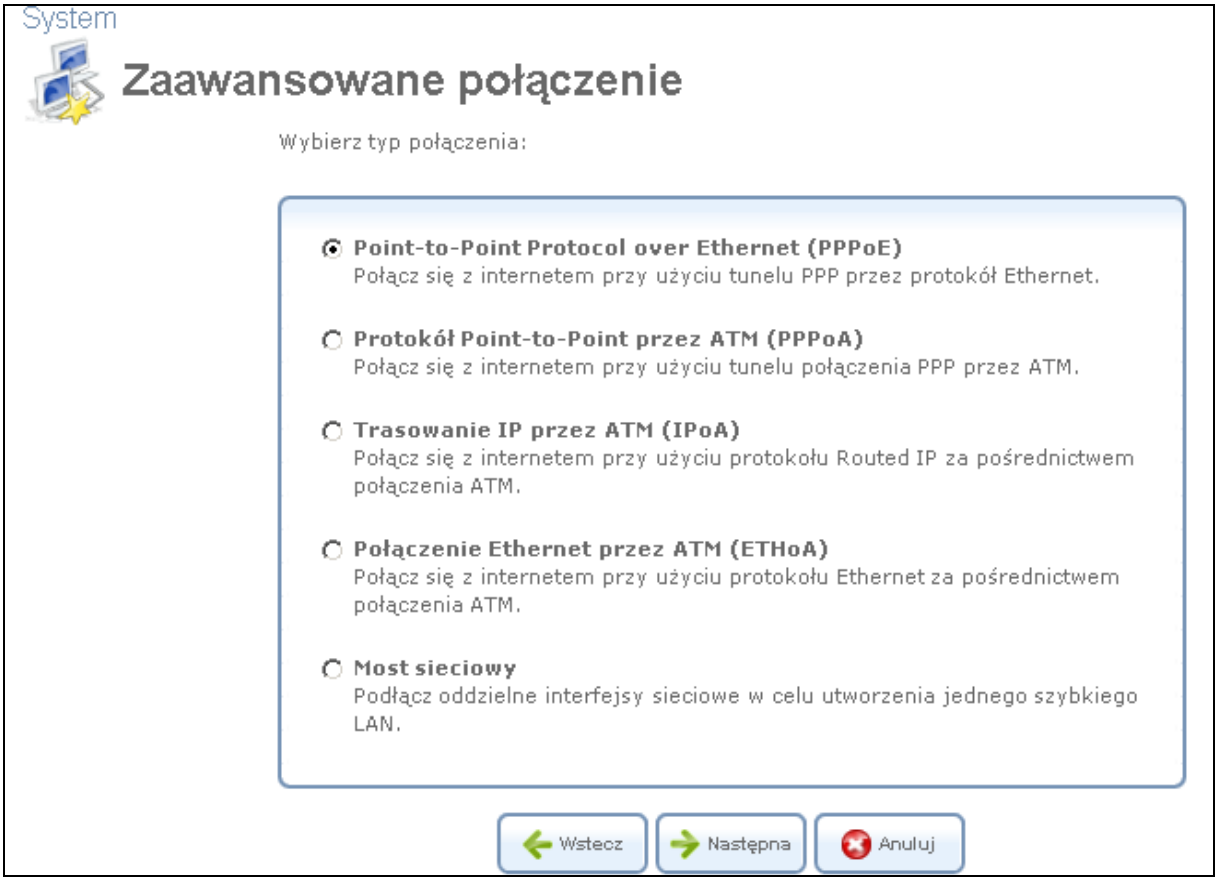
Rysunek 6.12 Kreator połączenia z internetem DSL

Opcje konfiguracji połączenia internetowego przedstawiono na rysunku 6.13, gdzie prostokąty reprezentują kroki/ekrany, które należy przejść, elipsy przedstawiają dostępne połączenia.



Rysunek 6.13 Drzewo kreatora połączeń internetowych

• Zaawansowane połączenie - Wybranie tej opcji powoduje przejście do sekcji „Połączenia zaawansowane", co pozwala na dobranie konfiguracji logicznej połączenia sieciowego. Ponadto kreator może tworzyć mosty sieciowe.

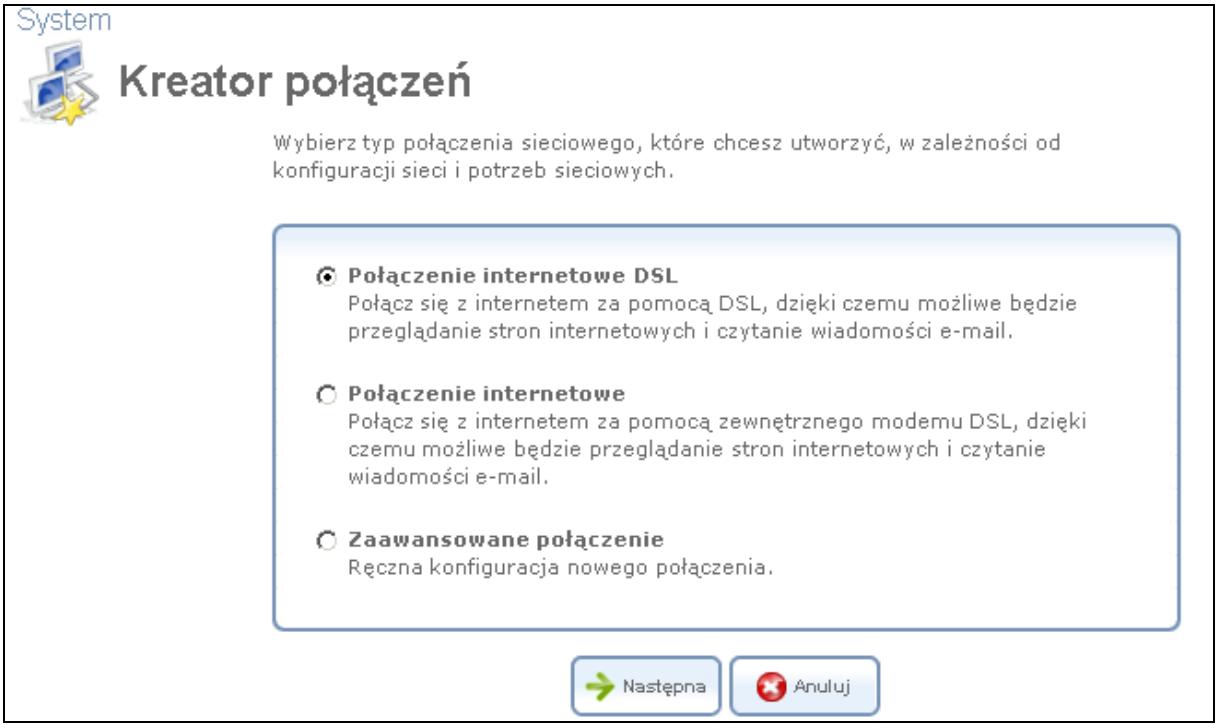


Rysunek 6.16 Zaawansowane połączenie

Zaawansowane opcje połączeń przedstawiono na rysunku 6.17.

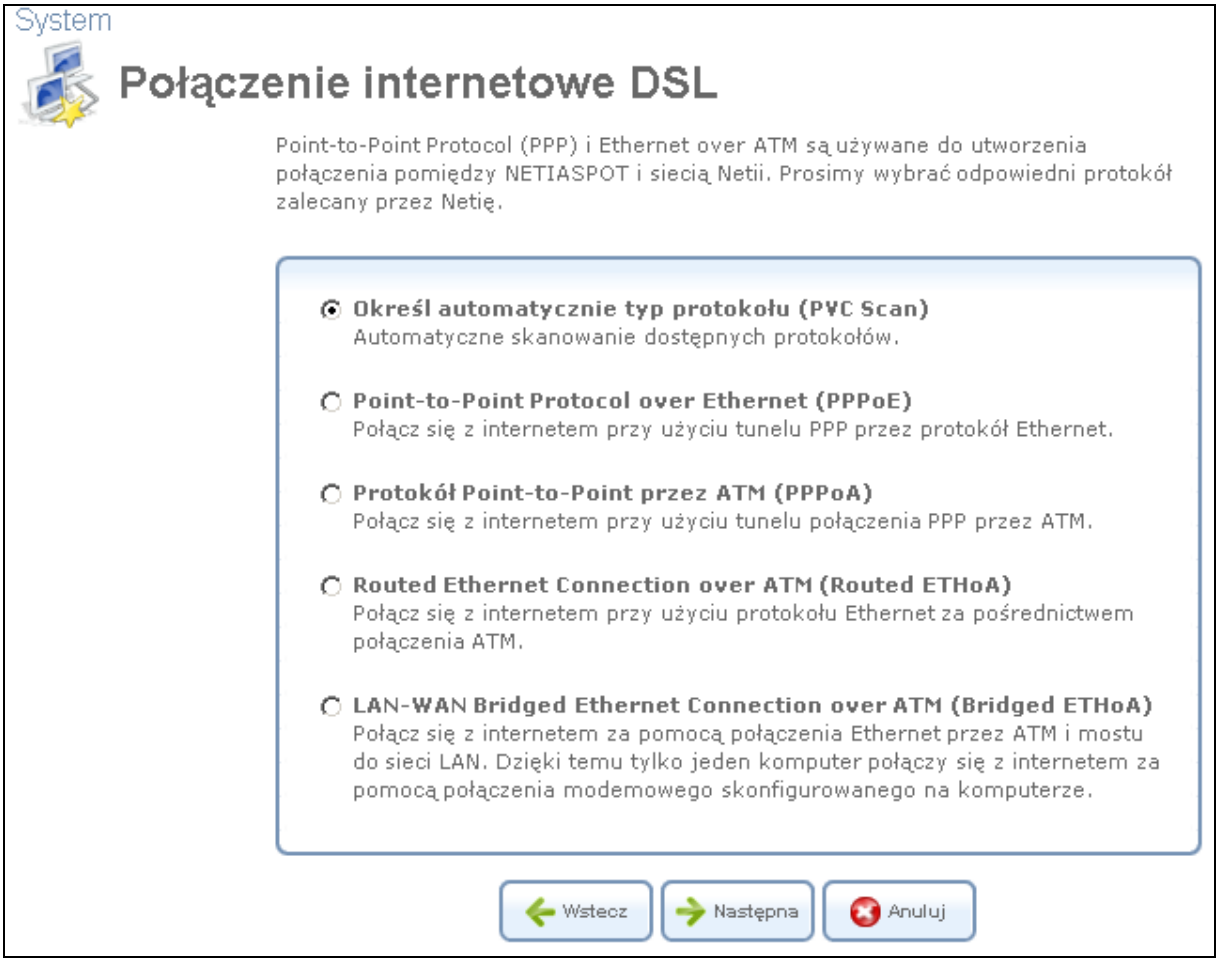
6.4.2.2. Tworzenie połączenia bramy DSL

Aby utworzyć nowe połączenie, kliknij przycisk link „Nowe połączenie" w ekranie „Połączenia sieciowe". Wyświetlony zostanie ekran „Kreator połączenia".



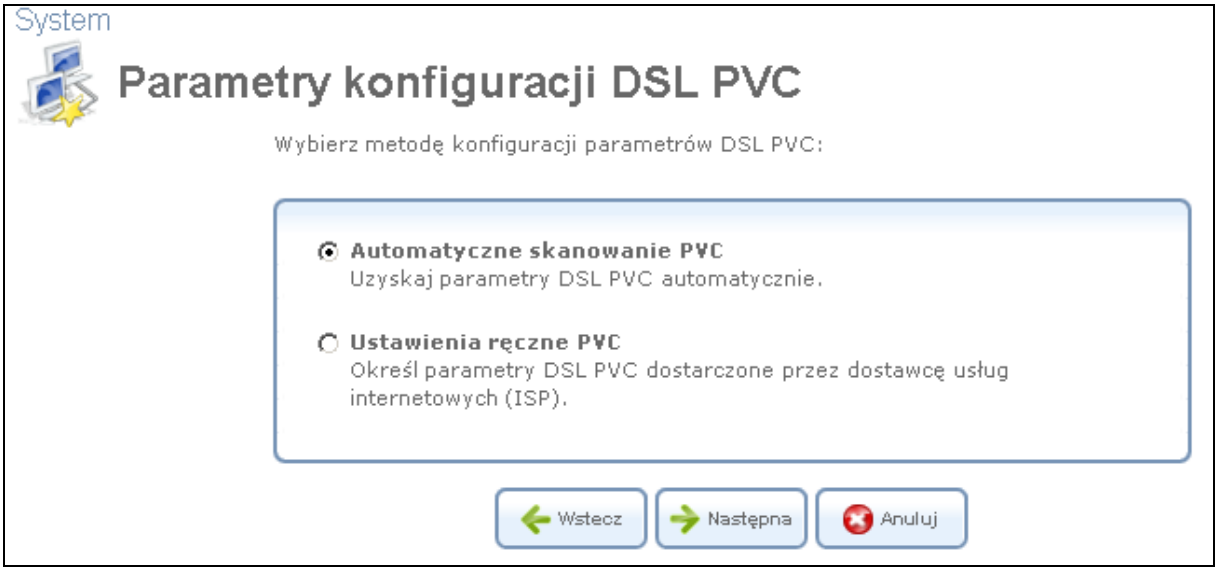
Rysunek 6.18 Kreator połączenia DSL

• Połączenie internetowe DSL - wybranie tej opcji spowoduje przejście do „Połączenie internetowe DSL" (patrz Rysunek 6.19), co pozwala skonfigurować połączenie z Internetem DSL przy użyciu jednej z dostępnych metod.



Rysunek 6.19 Kreator połączenia DSL

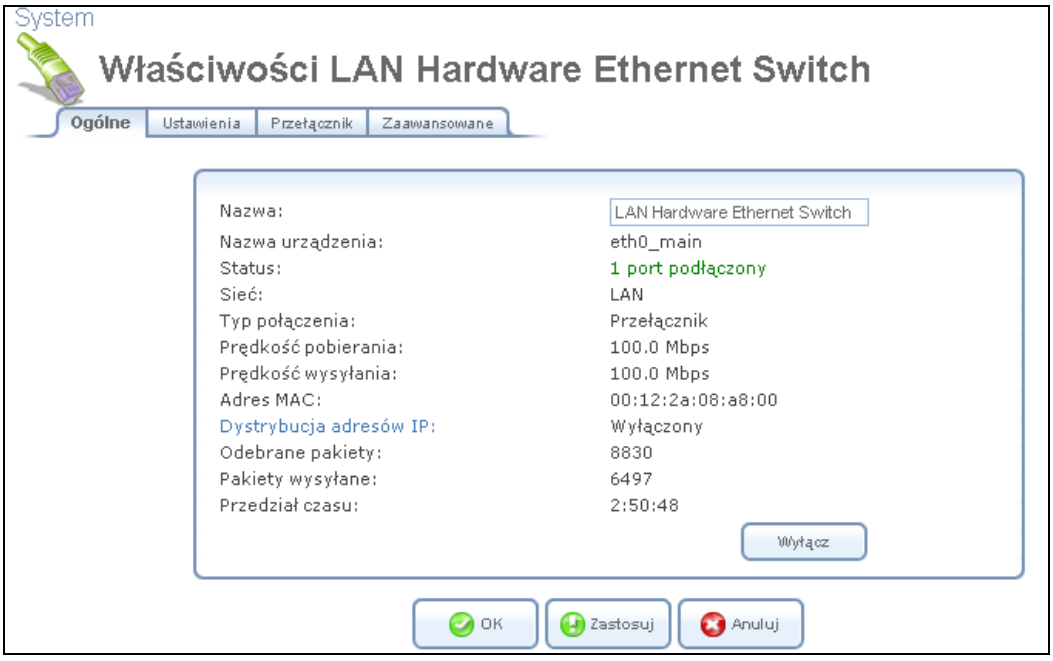
• Zaawansowane połączenie - wybranie tej opcji spowoduje przejście do sekcji „Połączenie zaawansowane" (patrz rysunek 6.20). Ta sekcja jest punktem wyjścia dla wszystkich połączeń DSL i zawiera dodatkowe połączenia, takich jak trasowanie IP przez ATM (IPoA) i most sieciowy.



Rysunek 6.20 Parametry konfiguracji DSL

6.4.3. Konfiguracja właściwości LAN Hardware Ethernet Switch

LAN Hardware Ethernet Switch reprezentuje wszystkie porty LAN OpenRG. Aby wyświetlić i zmodyfikować ustawienia sprzętowe „LAN Hardware Ethernet Switch", kliknij link „LAN Hardware Ethernet Switch" w sekcji „Połączenie sieciowe" (patrz rysunek 6.10). Wyświetlone zostaną zaawansowane opcje konfiguracyjne.



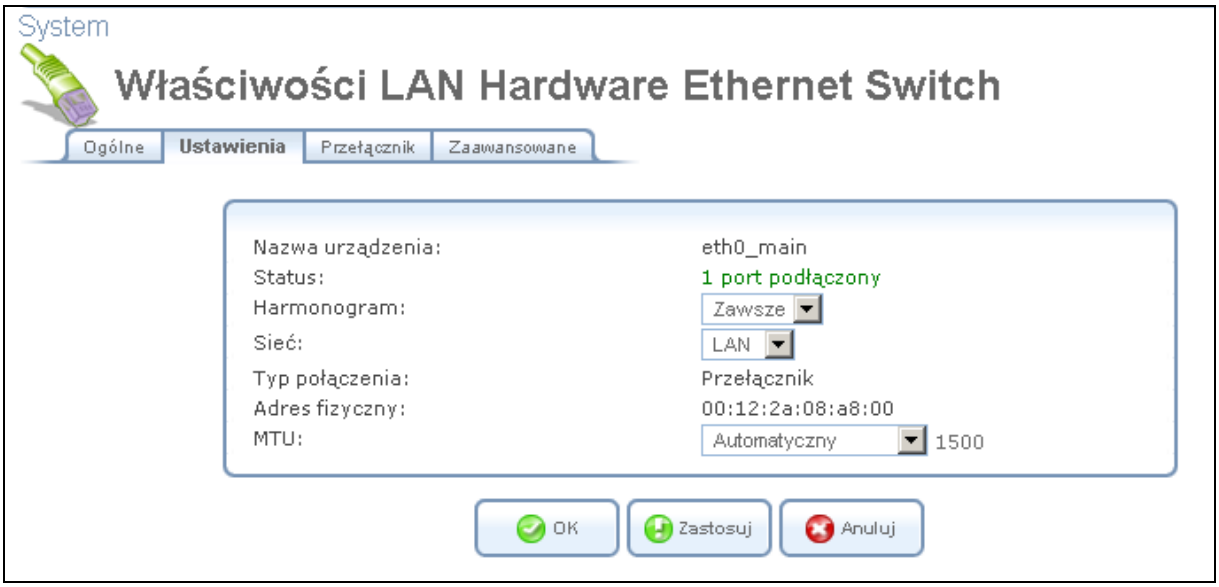
Rysunek 6.21 Właściwości LAN Hardware Ethernet Switch

6.4.3.1. Ogólne

Sekcja „Ogólne" umożliwia wyświetlanie sprzętu i ustawień LAN Ethernet Switch (patrz rysunek 6.21). Ustawienia te można edytować w pozostałej części ekranu, jak opisano poniżej.

6.4.3.2. Ustawienia

Sekcja wyświetla ogólne parametry połączenia. Zaleca się, aby nie zmieniać wartości domyślnych, chyba że jesteś zaznajomiony z pojęciami sieci, które reprezentują dane ustawienia. Brama jest skonfigurowana do pracy z wartościami domyślnymi, bez potrzeby modyfikacji parametru.



Rysunek 6.22 Ustawienia

Harmonogram - domyślnie połączenie jest zawsze aktywne. Jednakże, można skonfigurować zasady harmonogramu w celu określenia segmentów czasu, w którym połączenie może być aktywne. Po wybraniu zdefiniowanej reguły, z rozwijanego menu pozwala na wybór pomiędzy dostępnymi regułami. Aby dowiedzieć się, jak skonfigurować reguły harmonogramu, możemy odnieść się do „Definiowania reguł harmonogramu" w części administracyjnej instrukcji OpenRG.

Sieć - wybierz, czy parametry konfigurowane odnoszą się do połączenia WAN, LAN lub DMZ wybierając typ połączenia z rozwijanego menu. Aby uzyskać więcej informacji, odnoszących się do powyższej funkcji, możemy ich znaleźć w sekcji „Typy sieci" administracyjnej instrukcji OpenRG. Należy pamiętać, że przy definiowaniu połączenia sieci jako DMZ, należy także:

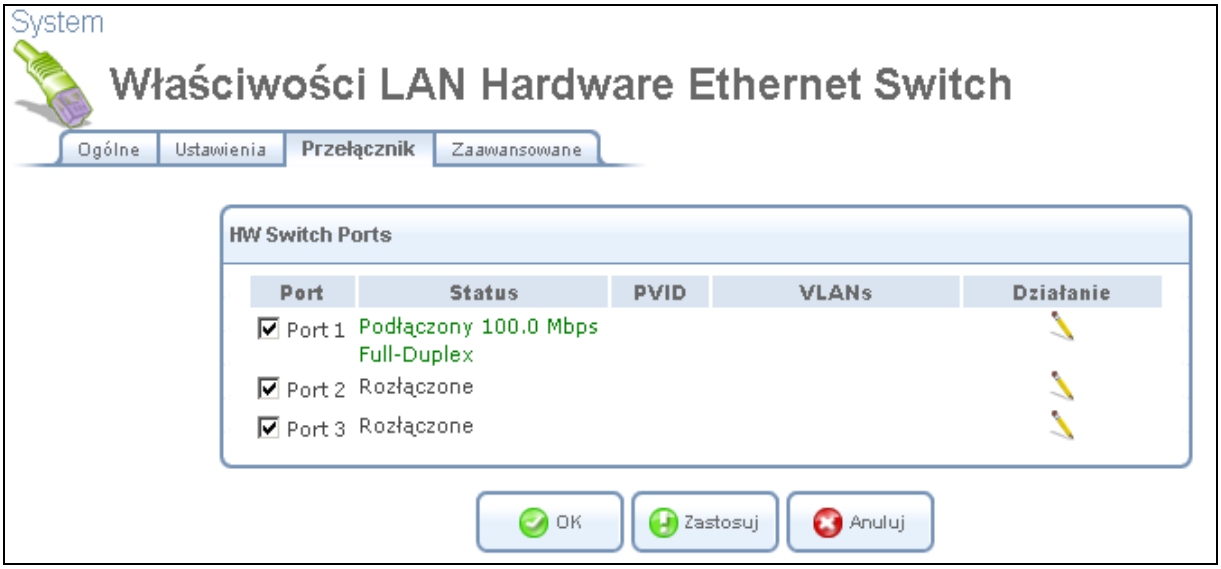
• Odłączyć połączenie z mostu, jeśli takie istnieje.
• Zmiana trybu połączenia trasy do „Router", w „Routingu".
• Dodaj reguły routingu na zewnątrz bramy (które mogą być dostarczane przez ISP), informuj sieć DMZ za OpenRG.

Adres fizyczny - adres fizyczny interfejsu sieciowego w sieci. Niektóre interfejsy pozwalają na zmianę tego parametru.

MTU - MTU jest to maksymalna jednostka transmisji. Określa ona największy rozmiar pakietu, jakim możemy przekazywać dane do Internetu. W ustawieniach domyślnych, automatycznie brama wybiera najlepsze MTU dla połączenia internetowego. Wybierz opcję „Automatycznie przez serwer DHCP", wtedy DHCP określenia wielkość MTU. W przypadku wybrania opcji „Ręcznie" zaleca się wpisać wartość od 1200 do 1500.

6.4.3.4 Przełącznik

Sekcja „Przełącznik" w karcie „Połączenia sieciowe" wyświetla właściwości sprzętowe portów przełącznika, fizycznych portów przełącznika, gniazda na płycie, do których stosuje się różne kable połączeniowe. Ten ekran składa się z listy dostępnych portów, ich statusu i sieci VLAN, której są członkami. Nieoznaczonych pakietów (pakiety bez znacznika VLAN), które kończą się w porcie, będą oznaczone z numerem VLAN, który pojawia się w sekcji „Identyfikator portu VLAN" (PVID).



Rysunek 6.23 Przełącznik

Możemy zmodyfikować konfigurację każdego portu. Aby to zrobić, kliknij ikonę działania połączonego portu. Wyświetlony zostanie ekran „Ustawienia portu LAN".

Rysunek 6.24 Ustawienia portu LAN

Stopień polityki - wybierz, czy przychodzące pakiety z portu będą znakowane w postaci nagłówka VLAN. Kiedy wybierzemy opcję „Tagowane" (Dodaj nagłówek VLAN), pojawiają się dodatkowe pola.

Domyślny VLAN ID – identyfikator portu VLAN. Możesz dodać dodatkowe identyfikatory VLAN, klikając przycisk „Nowy wpis".

6.4.3.5 Zaawansowane

W tej sekcji możemy skonfigurować następujące zaawansowane opcje przełącznika.

• Zapora połączenia internetowego - zapora sieciowa na OpenRG pomaga chronić komputer poprzez zapobieganie nieautoryzowanym użytkownikom i uzyskania dostępu do niego za pośrednictwem sieci, takiej jak Internet. Zapora może być aktywowany za pomocą połączenia z siecią. Aby włączyć zaporę na aktualnym połączeniu sieciowym, wybierz pole wyboru „Włączony". Aby dowiedzieć się więcej o zabezpieczeniach OpenRG, patrz punkt 5.2.

Rysunek 6.25 Zapora połączenia internetowego

Połączenie internetowe FastPath - zaznaczenie tego pola wyboru wykorzysta algorytm FastPath dla zwiększenie przepływu pakietów, co skutkuje szybszą komunikację pomiędzy siecią LAN i WAN. Domyślnie ta funkcja jest włączona.

Rysunek 6.26 Internet FastPath

• Dodatkowe adresy IP - można dodać aliasy (dodatkowe adresy IP) bramy, klikając link „Nowy adres IP". Ta opcja pozwala na dostęp do bramy przy użyciu tych aliasów w uzupełnieniu do domyślnego 192.168.1.254 i http://netiaspot.home

Rysunek 6.27 Dodatkowe adresy IP

6.4.4. Konfiguracja mostu sieciowego LAN

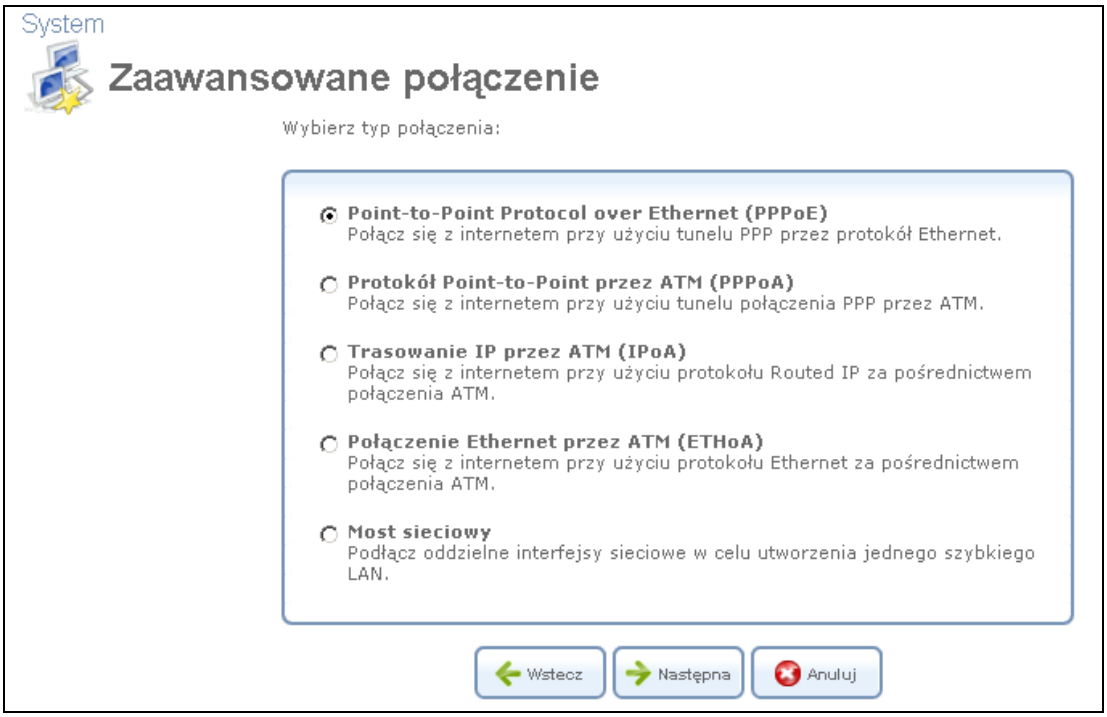
Połączenie mostu sieciowego LAN służy do łączenia kilku urządzeń w ramach jednej wirtualnej sieci LAN. Na przykład, gdy tworzymy jedną sieć Ethernet LAN w połączeniu z bezprzewodową siecią LAN. Należy pamiętać, że most zostanie usunięty, jego podstawowe wcześniejsze ustawienia DHCP dziedziczą urządzenia, dawniej podłączone do mostu. Na przykład, usunięcie mostu, który jest skonfigurowany jako klient DHCP, automatycznie konfiguruje urządzenia LAN dawniej stanowiące most sieciowy jako klientów DHCP, z dokładną konfiguracją klienta DHCP.

6.4.4.1 Tworzenie sieci LAN Połączenie mostkowe

Aby utworzyć nowy most lub skonfigurować już istniejący, wykonaj następujące czynności:

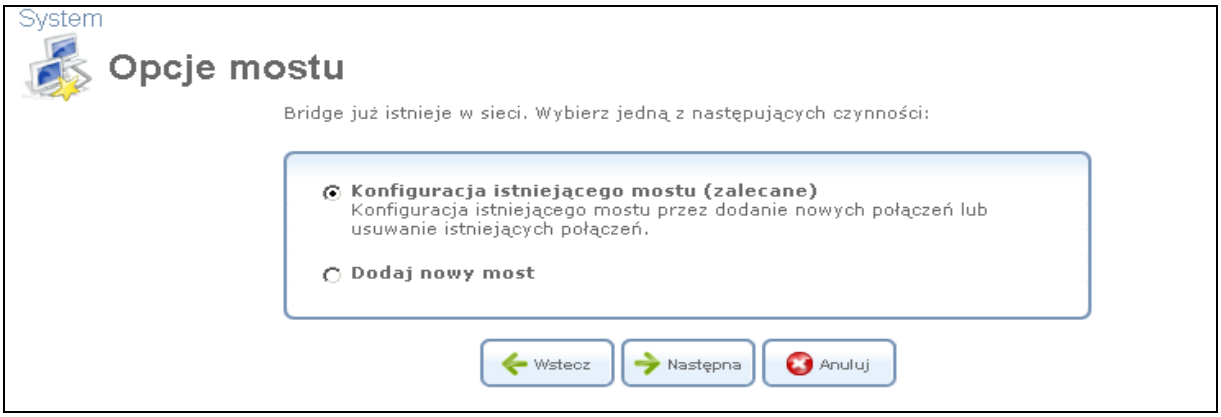
1. W sekcji „Połączenia sieciowe" w menu „System" (patrz rysunek 6.10), kliknij link „Nowe połączenie". Wyświetlony zostanie ekran „Kreator połączeń" (patrz rysunek 6.11, 6.18).

2. Wybierz opcję „Zaawansowane połączenie", a następnie przycisk „Dalej". Wyświetlony zostanie ekran „Zaawansowane połączenie".



Rysunek 6.28 Kreator zaawansowanej konfiguracji

3. Wybierz przycisk „Most sieciowy”, a następnie przycisk „Dalej”. Wyświetlony zostanie ekran „Opcje mostu”.



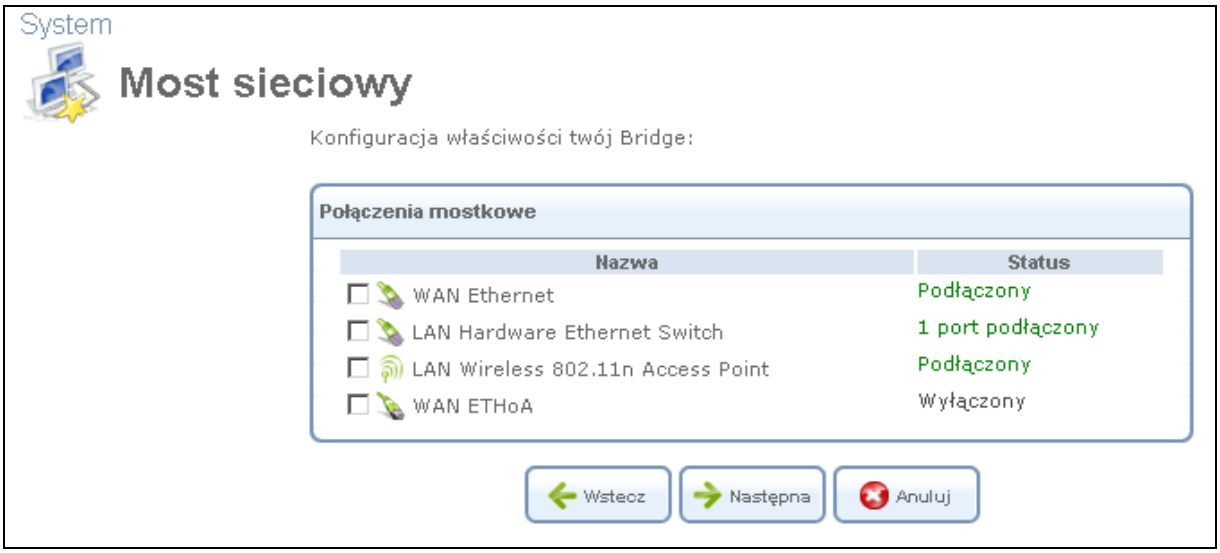
Rysunek 6.29 Opcje mostu

4. Wybierz, czy chcesz modyfikować konfigurację istniejącego mostu (ta opcja pojawi się tylko jeśli most istnieje) lub dodać nowy most:

a. **Konfiguracja istniejącego mostu** - wybierz tą opcję i kliknij „Dalej”. Ekran „Most sieciowy” wyświetla aktualne połączone interfejsy i pozwala na dodawanie nowych połączeń do mostu lub pozwala usunąć istniejące przez ich zaznaczenie lub usuwając zaznaczenie pól wyboru. Na przykład, aby utworzyć most WAN-LAN, wybierz połączenie WAN z pola wyboru.

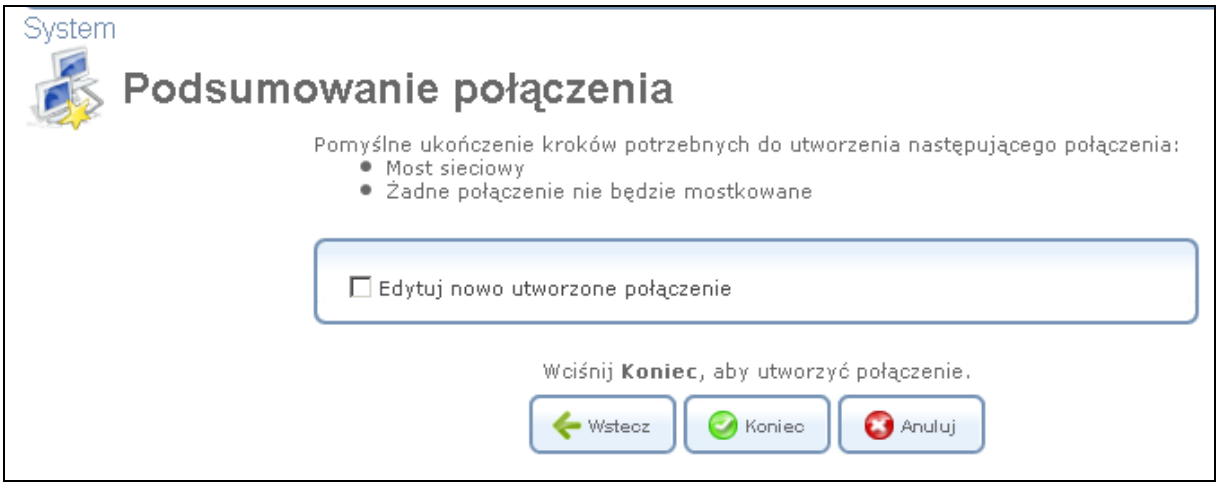
Rysunek 6.30 Most sieciowy – konfiguracja istniejącego mostu

b. Wybierz opcję „Dodaj nowy most sieciowy” i kliknij „Dalej”. W nowym oknie dialogowym zostaną wyświetlone możliwe do połączenia interfejsy sieciowe przez wybór odpowiednich pól wyboru.



Rysunek 6.31 Most sieciowy – dodanie nowego mostu sieciowego

5. Kliknij przycisk „Dalej”. Wyświetlony zostanie ekran „Podsumowanie połączenia”, wyświetlając odpowiednie zmiany.



Rysunek 6.32 Podsumowanie połączenia – konfiguracja istniejącego mostu

6. Wybierz pole wyboru „Edytuj nowo utworzone połączenie”, jeśli chcesz być skierowany do nowego ekranu konfiguracji połączenia po kliknięciu przycisku „Zakończ”. Ekran ten jest opisany w dalszej części tego rozdziału.

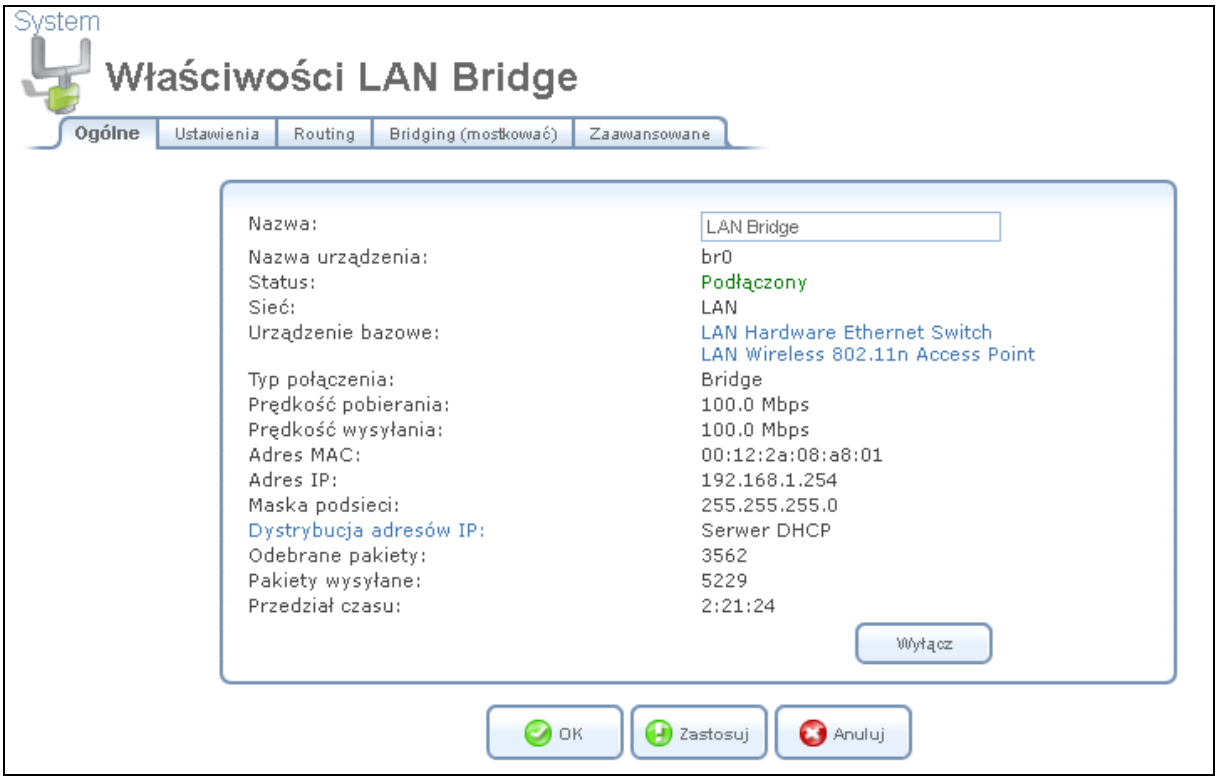
7. Kliknij przycisk "Zakończ ", aby zapisać ustawienia. Nowy most zostanie dodany do listy połączeń sieci i będzie konfigurowalny, jak każdy inny most.

Nowy most zostanie dodany do listy połączeń sieciowych i będziemy mogli go konfigurować,
jak każdy inny most.

Uwaga: Utworzenie mostu sieciowego WAN-LAN wyłącza serwer DHCP OpenRG. Oznacza to, że komputery z sieci lokalnej mogą otrzymać adresu IP z serwera DHCP w sieci WAN. Jeśli skonfigurujemy hosta ze statycznym adresem IP z adresem podsieci mostu (192.168.1.x), będziemy mogli uzyskać dostęp do OpenRG, ale nie WAN, ponieważ NAT nie jest wykonywany w trybie mostu sieciowego WAN-LAN.

6.4.4.2. Przeglądanie i edytowanie ustawień mostu sieciowego LAN

Po utworzeniu mostu, można wyświetlić lub zmodyfikować jego ustawienia, klikając na link „Połączenia sieciowe" i następnie na link wybranego mostu sieciowego.



Rysunek 6.33 Właściwości mostu sieciowego

6.4.4.2.1. Ogólne

Ta sekcja wyświetla kartę umożliwiającą wyświetlanie ustawień sieci LAN połączenia mostu sieciowego (patrz rysunek 6.33). Te ustawienia mogą być edytowane w pozostałej części ekranu i zakładek podrzędnych, jak opisano w następujących sekcjach.

6.4.4.2.2. Ustawienia

Ta karta pozwala modyfikować następujące ustawienia mostu sieciowego LAN.

Ogólne - ta sekcja wyświetla ogólne parametry połączenia. Zaleca się nie zmieniać wartości domyślnych, chyba że jesteś zaznajomiony z pojęciami zawartymi w powyższej sekcji. Ponieważ brama jest skonfigurowana do pracy z wartościami domyślnymi, bez dodatkowych parametrów nie jest konieczne wprowadzenie modyfikacji parametrów domyślnych.

Rysunek 6.34 Ustawienia interfejsu

Harmonogram - domyślnie połączenie jest zawsze aktywne. Jednakże, można skonfigurować zasady harmonogramu w celu określenia przedziałów czasu, w którym połączenie może być aktywne. Zdefiniowane reguły harmonogramu, możemy wybierać z rozwijanego menu, spośród dostępnych reguł. Aby dowiedzieć się, jak skonfigurować reguły harmonogram możemy odnaleźć w sekcji „Definiowanie reguł harmonogramu" administracyjnej instrukcji OpenRG.

Sieć - wybieramy czy parametry konfiguracyjne odnoszą się do połączenia WAN, LAN lub DMZ, wybierając typ połączenia z rozwijanego menu. Aby uzyskać więcej informacji

znajdujących się w sekcji „Typy sieci" administracyjnej instrukcji OpenRG. Należy pamiętać, że przy definiowaniu połączenia sieci DMZ, należy także:

• Odłączyć połączenie z mostu, jeśli takie istnieje.
• Zmiana trybu połączenia trasy do „Router", w „Routingu".
• Dodaj reguły routingu na zewnątrz bramy (które mogą być dostarczane przez ISP), informuj sieć DMZ za OpenRG.

Adres fizyczny - adres fizyczny interfejsu sieciowego w sieci. Niektóre interfejsy pozwalają na zmianę tego parametru.

MTU - MTU jest to maksymalna jednostka transmisji. Określa ona największy rozmiar pakietu, jakim możemy przekazywać dane do Internetu. W ustawieniach domyślnych, automatycznie brama wybiera najlepsze MTU dla połączenia internetowego. Wybierz opcję „Automatycznie przez serwer DHCP", wtedy DHCP określenia wielkość MTU. W przypadku wybrania opcji „Ręcznie" zaleca się wpisać wartość od 1200 do 1500.

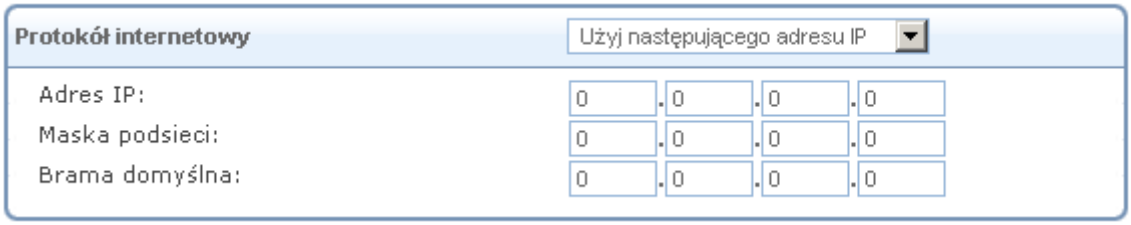
Protokół internetowy - wybierz jedną z następujących opcji protokołu internetowego z rozwijanego menu „Protokół internetowy":
• Brak adresu IP
• Użyj następującego adresu IP

Należy pamiętać, że ekran zostanie odświeżony, aby wyświetlić odpowiednie ustawienia w zależności od wyboru.

Brak adresu IP - wybierz „Brak adresu IP", jeśli wymaga się, żeby brama nie posiadała adresu IP. Opcja ta może być użyteczna, jeśli pracujesz w środowisku, w które nie jest podłączone do innych sieci, takich jak Internet.

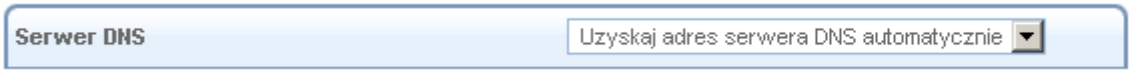
Rysunek 6.35 Protokół internetowy - Brak adresu IP

Użyj następującego adresu IP - połączenie można skonfigurować za pomocą stałego (statycznego) adresu IP. Usługodawca powinien zapewnić wtedy taki adresu IP i maskę podsieci.



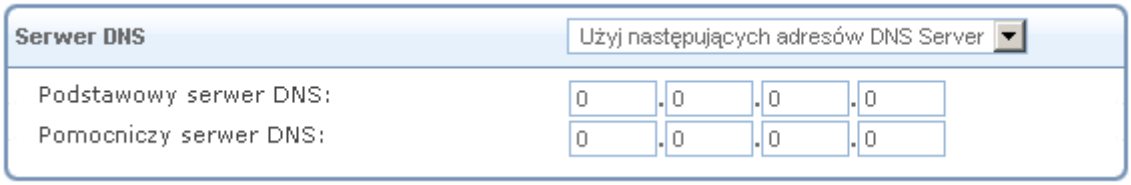
Rysunek 6.36 Protokół internetowy – Statyczne IP

Serwer DNS - Domain Name System (DNS) jest metodą, w której nazwy domeny witryny sieci www, są tłumaczone na adresy IP. Możesz skonfigurować połączenie do automatycznego uzyskania adresów serwera DNS, albo określić takiego adresy ręcznie, zgodnie z informacjami dostarczanymi przez ISP. Aby skonfigurować połączenie do automatycznego uzyskania serwera DNS, wybierz opcję „Uzyskaj adres serwera DNS automatycznie" z rozwijanego menu „Serwer DNS".



Rysunek 6.37 Serwer DNS – Automatyczne uzyskiwanie parametrów

Aby ręcznie skonfigurować adresy serwerów DNS, wybierz opcję „Użyj następujących serwerów DNS" z rozwijanego menu (patrz rysunek „Serwer DNS - Statyczne IP"). Określ do dwóch różnych adresów serwera DNS, pierwotny i zapasowy.



Rysunek 6.38 Serwer DNS - Statyczne IP

Dystrybucja adresów IP - sekcja „Dystrybucja adresów IP" pozwala skonfigurować serwer „Dynamic Host Configuration Protocol" (DHCP). Serwer DHCP automatycznie przypisuje

adresy IP do komputerów w sieci. Po włączeniu tej funkcji, upewnij się, że także komputery są skonfigurowane jako klienci DHCP. Obszerny opis tej funkcji, patrz punkt 5.6. Wybierz jedną z następujących opcji z rozwijanego menu „Dystrybucja adresów IP":

Serwer DHCP

W przypadku wybranego serwera DHCP, należy wpisać następujące pola:

Początkowy adres IP - pierwszy adres IP, który może być przydzielony do komputera LAN. Domyślny adres interfejsu LAN to 192.168.1.254, zaleca się, żeby pierwszy adres IP przypisany do hosta sieci LAN to 192.168.1.2 lub wyżej.

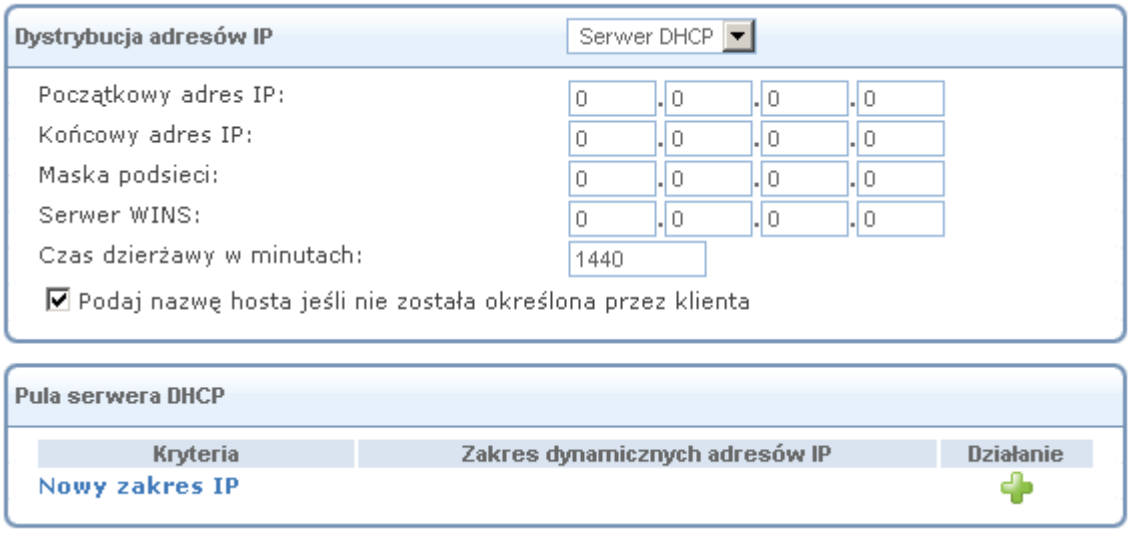
Końcowy adres IP - końcowy adres IP z zakresu, który może być używany do automatycznego przypisywania adresów IP do komputerów z sieci lokalnej.

Maska podsieci -maska służy do określenia, do jakiej podsieci należy adres IP. Przykładowa domyślna wartość maski podsieci to 255.255.255.0.

Serwer WINS - jeśli chcesz korzystać z zewnętrznego serwera WINS, należy wpisać jego adres IP i kliknąć „OK".

Czas dzierżawy w minutach - każdemu urządzeniu będzie przypisany adres IP przez serwer DHCP na określony czas, gdy łączy się z siecią. Po wygaśnięciu dzierżawy serwer będzie ustalał, czy komputer jest odłączony od sieci. Jeśli tak, serwer może przypisać adres IP do komputera nowo podłączonego. Funkcja ta zapewnia, że adresy IP, które nie są w użyciu będą dostępne dla innych komputerów w sieci.

Podaj nazwę hosta jeśli nie zostanie podana przez klienta - jeśli klient DHCP nie ma nazwy hosta, brama będzie automatycznie przypisać taką nazwę dla niego.



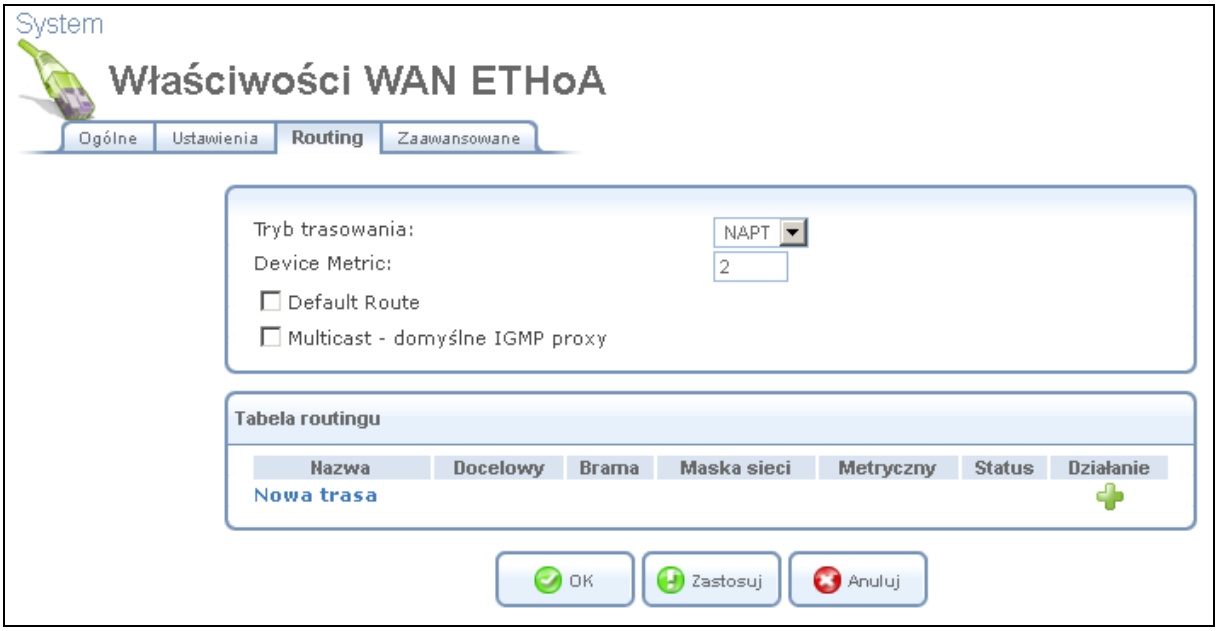
Rysunek 6.39 Dystrybucja adresów IP – Serwer DHCP

Wyłączony - wybierz opcję „Wyłączony" z rozwijanego menu, jeśli chcieliby Państwo statycznie przypisać adresy IP do komputerów w sieci.

Rysunek 6.40 Dystrybucja adresów IP – Wyłączone DHCP

6.4.4.2.3. Routing

Ta zakładka umożliwia skonfigurowanie ustawień trasowania połączenia. Można wybrać i skonfigurować bramę do statycznego lub dynamicznego routingu. Routing dynamiczny automatycznie dostosowuje tablice trasowania do ruchu pakietów w sieci. Routing statyczny określa stałą ścieżkę do innych podsieci.



Rysunek 6.41 Zaawansowane właściwości trasowania

Możesz skonfigurować następujące ustawienia:

Tryb trasowania - wybierz jeden z następujących trybów trasy:

Trasa - użyj tej funkcji, jeśli chcesz , aby brama działania jako router między dwoma sieciami.

NAPT - Network Address Port Translation (NAPT) odnosi się do procesu translacji adresów z udziałem mapowania numerów portów, dzięki czemu wiele maszyn przy posiadaniu jednego publicznego adresu IP. Użyj NAPT, jeśli LAN obejmuje wiele urządzeń, topologii, które wymagają tłumaczenia port oprócz translacji adresów.

Device metric (metryka urządzenia) - jest wartością używaną przez bramę w celu określenia, czy jedna trasa jest lepsza od innej, biorąc pod uwagę takie parametry jak przepustowość, opóźnienie i wiele innych.

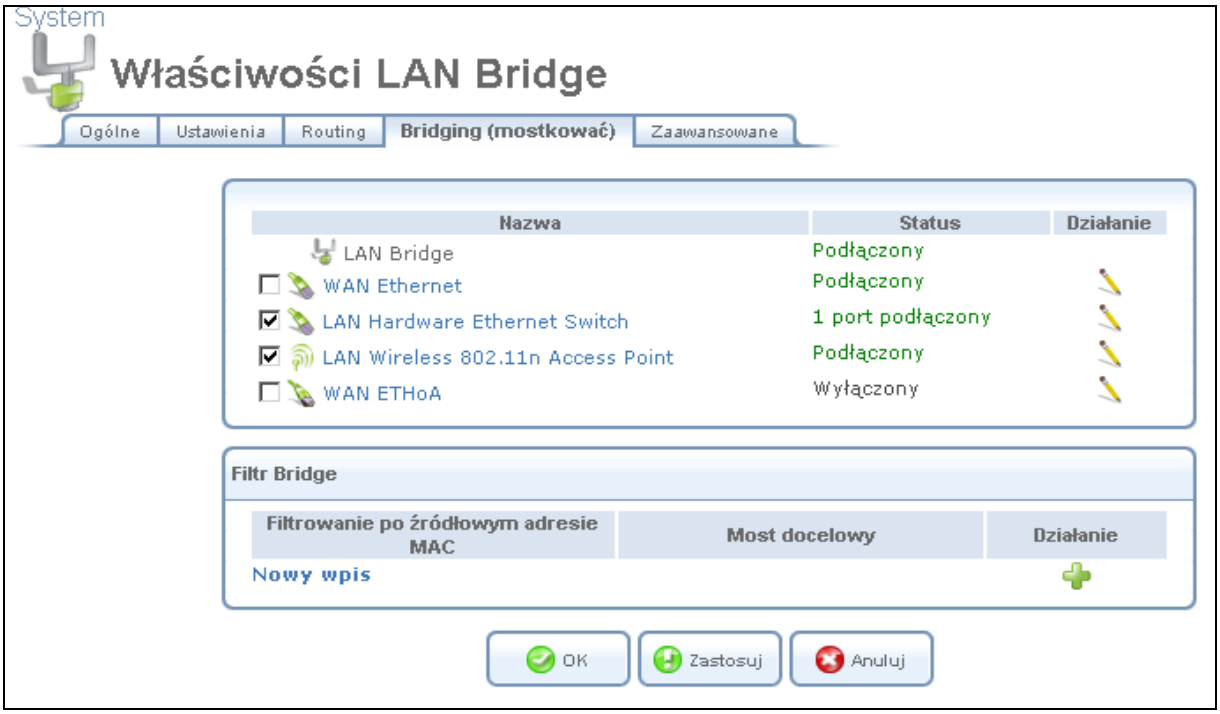
Trasa domyślna - zaznacz to pole wyboru w celu określenia tego urządzenia jako domyślnej trasy.

Multicast - domyślne proxy IGMP - OpenRG służy jako serwer proxy IGMP, wydawanie przyjmowanych komunikatów IGMP w imieniu podłączonych komputerów z sieci lokalnej. To pole wyboru jest aktywne domyślnie w sieci LAN, co oznacza, że jeśli serwer multicast jest dostępny w LAN, inne komputery z sieci LAN wyślą prośbę, aby dołączyć do grup multicast (wyślą żądanie IGMP). Jednak to pole wyboru jest wyłączone domyślnie dla połączenia WAN, co oznacza, że komputery z sieci lokalnej nie będą w stanie dołączyć do grupy multicast WAN serwerów multicast. Podczas tworzenia mostu sieciowego WAN-LAN, to pole wyboru musi być odznaczone.

Wersja IGMP Query - OpenRG obsługuje wszystkie trzy wersje IGMP. Wybierz wersję, której chcesz użyć. Pamiętaj, że menu rozwijane pojawia się tylko podczas połączenia LAN.

Tabela routingu - umożliwia dodanie lub zmianę trasy, gdy urządzenie jest aktywne. Użyj przycisku „Nowa trasa", aby dodać trasy lub edytować istniejące trasy.

6.4.4.2.4. Mostkowanie interfejsów



Rysunek 6.42 ustawienia mostu LAN

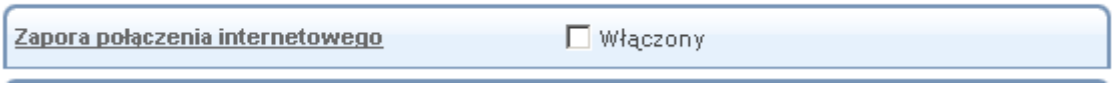
Filtr mostu (bridge) - sekcja jest używana do tworzenia reguł filtrowania ruchu na moście sieciowym, w celu aby umożliwiać bezpośredni przepływ pakietów między siecią WAN i LAN. Takim przykładem jest ustalanie trybu mostka hybrydowego (patrz punkt 6.4.13.2).

Sprzętowe przyspieszenie mostu (Bridge hardware acceleration) - zaznaczenie tego pola wyboru wykorzysta algorytm FastPath dla zwiększenia przepływu pakietów przez most sieciowy. Należy pamiętać, że ta funkcja musi być wspierana i aktywna po obu stronach mostu, aby funkcja działała poprawnie.

6.4.4.2.5 Zaawansowane

Ta sekcja pozwala skonfigurować ustawienia zaawansowane mostu LAN.

• **Zapora połączenia internetowego** - Twoja zapora sieciowa urządzenia pomaga chronić komputer poprzez zapobieganie nieautoryzowanym uzyskaniem dostępu przez użytkowników za pośrednictwem sieci, takiej jak Internet. Zapora sieciowa może być aktywowana na danym połączeniu sieciowym. Aby włączyć zapory dla połączenia sieciowego, zaznacz pole wyboru „Włączony". Aby dowiedzieć się jak najwięcej na temat zabezpieczeń bramy, patrz punkt 5.2.



Rysunek 6.43 Zapora połączenia internetowego

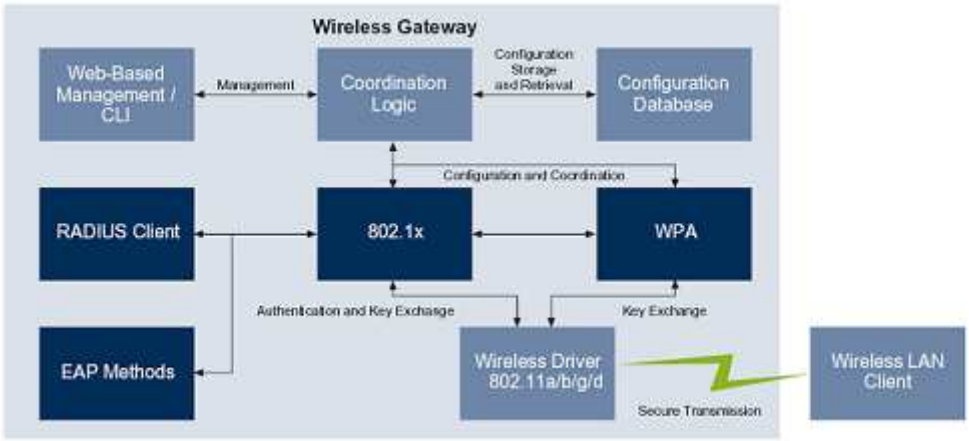
• **Dodatkowe adresy IP** - można dodać aliasy (dodatkowe adresy IP) bramy, klikając na link „Nowy adres IP". Pozwala to dostępu do bramy za pomocą aliasów oprócz domyślnego 192.168.1.254 i http://netiaspot.home.

Rysunek 6.44 Dodatkowe adresy IP

6.4.5. Konfiguracja sieci bezprzewodowej

OpenRG zapewnia szerokopasmowe urządzenie abonenckie (CPE). Kompletne oprogramowanie do tworzenia łączności bezprzewodowej w standardzie 802.11b/g/n. Rozwiązanie jest zintegrowane i obejmuje działania systemu, protokołów komunikacyjnych, tras, zaawansowane funkcje sieci bezprzewodowej i szerokopasmowej, bezpieczeństwa, zdalnego zarządzania oraz aplikacji sieciowych w domu.

OpenRG integruje kilka warstw zabezpieczeń sieci bezprzewodowych. Należą do nich IEEE 802.1x w oparciu o protokół uwierzytelniania, klienta RADIUS, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, Wi-Fi Protected Access (WPA), WPA2, WPA i WPA2 (tryb połączony), jak również zaporę sieciową OpenRG i aplikacje VPN. Ponadto OpenRG posiada wbudowany serwer uwierzytelniania użytkowników w domu czy biurze, określa autoryzowanych, bezprzewodowych użytkowników bez potrzeba zewnętrznego serwera RADIUS.

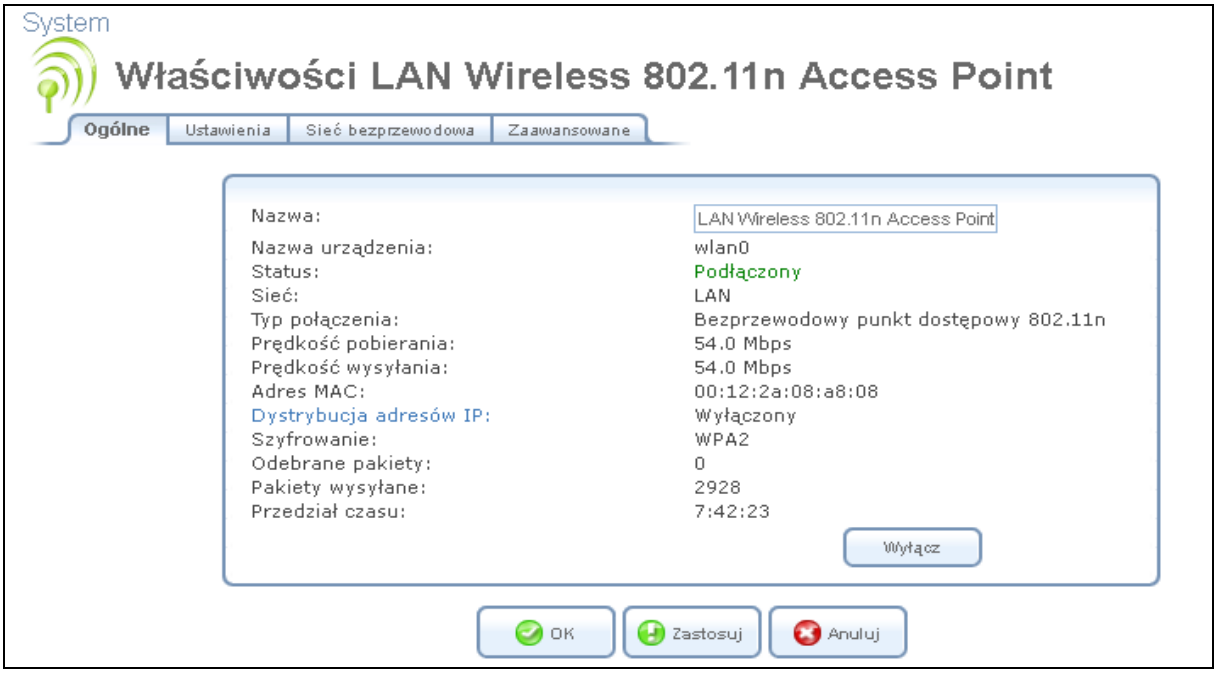


Rysunek 6.45 Komponenty uwierzytelniania i szyfrowania sieci bezprzewodowej OpenRG

6.4.5.1 Włączenie w OpenRG interfejsu sieci bezprzewodowej

Aby włączyć interfejs bezprzewodowy sieci OpenRG, wykonaj następujące czynności:

1. Kliknij link „LAN 802.11n Access Point" w sekcji „Połączenia sieciowe" (patrz rysunek 6.10). Ekran „Właściwości Wireless LAN Access Point 802.11n" zostanie wyświetlony.

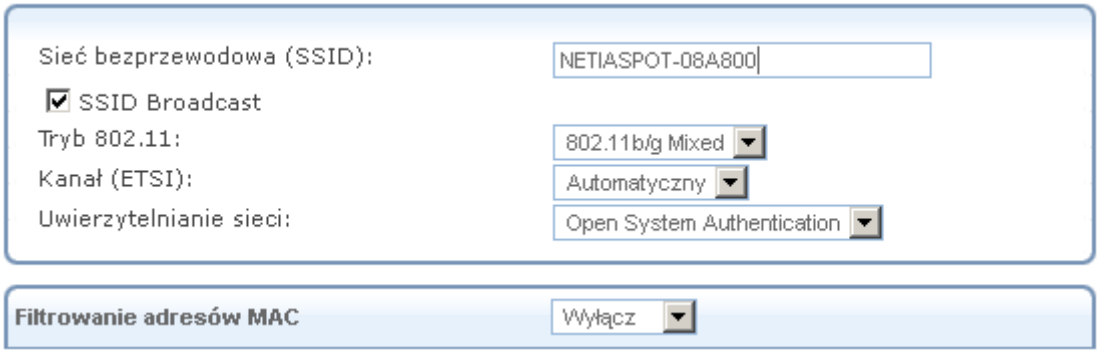


Rysunek 6.46 Właściwości wbudowanego punktu sieci bezprzewodowej 802.11n

2. Kliknij „Włącz" (ten przycisk jest wyświetlany tylko wtedy, gdy punkt bezprzewodowy jest dostępny w naszym urządzeniu). Po odświeżeniu ekranu, po zmianie stanu połączenia na „Podłączony". Domyślnie wbudowany punkt bezprzewodowy jest włączony.

3. Kliknij przycisk „Sieć bezprzewodowa" w zakładce „Połączenia sieciowe".

4. W polu „SSID", można zmienić wyświetlaną nazwę sieci bezprzewodowej z domyślnej nazwy na bardziej indywidualną.



Rysunek 6.47 Punkt dostępowy sieci bezprzewodowej

5. Kliknij przycisk "OK ", aby zapisać ustawienia.

6.4.5.2 Zabezpieczenie sieci bezprzewodowej

Sieć bezprzewodowa OpenRG jest gotowa do pracy z wartościami domyślnymi. Poniżej w sekcji zabezpieczeń opisano, jak zabezpieczyć połączenie bezprzewodowe przy użyciu protokołu bezpieczeństwa WiFi Protected Access (WPA). Wi-Fi Alliance utworzony protokół zabezpieczeń WPA jako metodę szyfrowania danych w lokalnych sieciach bezprzewodowych 802.11 (WLAN). WPA jest protokołem wspierającym, normy wersji 802.11i z wykorzystaniem „Temporal Key Integrity Protocol" (TKIP), który rozwiązuje problemy „Wired Equivalent Privacy" (WEP), w tym wykorzystywanie dynamicznych kluczy.

6.4.5.2.1 Zabezpieczenie WPA

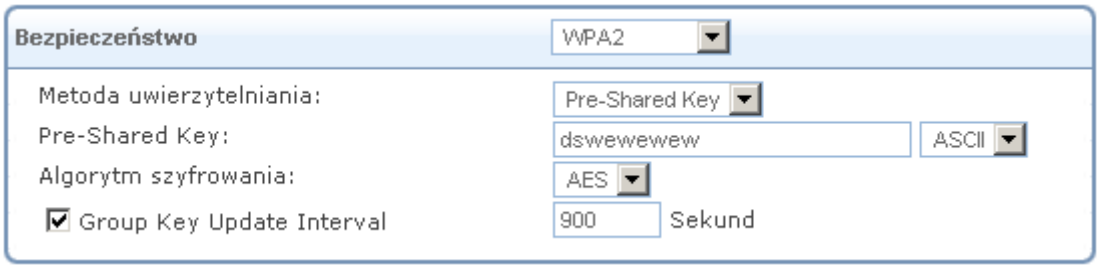
W celu zabezpieczenia sieci bezprzewodowej WPA, wykonaj następujące czynności:

1. Kliknij link „LAN 802.11n Access Point" na ekranie „Połączenia sieciowe".

Ekran „Właściwości LAN 802.11n Access Point" zostaną wyświetlone na następującym ekranie:

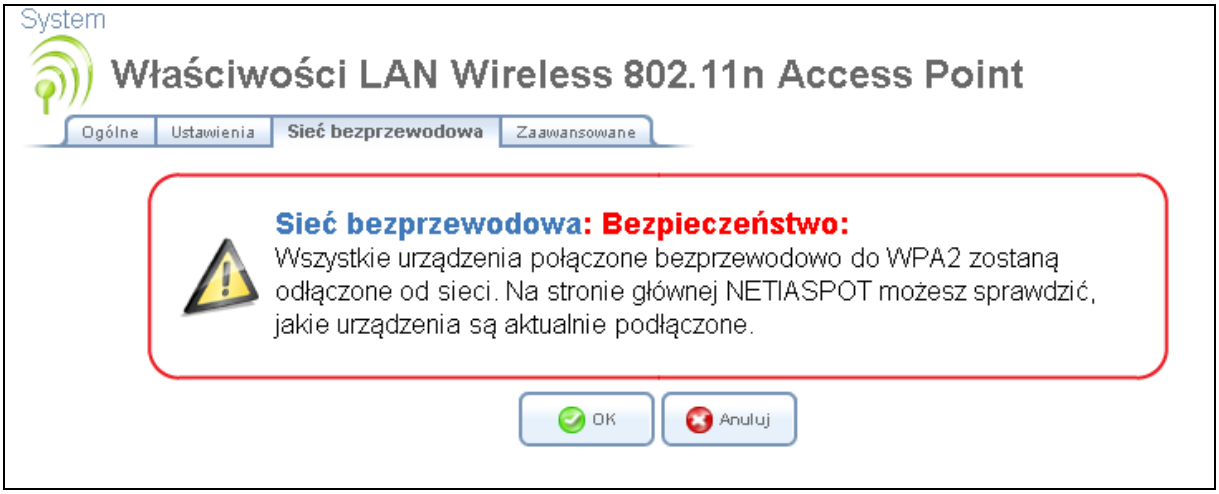
Rysunek 6.48 Sekcja ogólna konfiguracji sieci bezprzewodowej

2. Kliknij przycisk „Sieć bezprzewodowa” w zakładce właściwości sieci bezprzewodowej.
3. Z rozwijanego menu „Bezpieczeństwo”, należy wybrać „WPA”. Należy pamiętać, że przy wyborze WPA, zarówno WPA i WPA2 są obsługiwane.
4. Sprawdź, czy wybrana jest metoda uwierzytelniania „Pre-Shared Key”.
5. W polu tekstowym „Pre-Shared Key” wpisz co najmniej 8 znaków. Upewnij się, że wybrana jest z rozwijanego menu opcja „ASCII”.



Rysunek 6.49 Parametry bezpieczeństwa WPA

6. Kliknij przycisk „OK”. Następnie wyświetlony zostanie ekran „Uwaga”.



Rysunek 6.50 Ostrzeżenie o rozłączeniu klientów sieci bezprzewodowej

7. Kliknij przycisk „OK”, aby zapisać ustawienia.

6.4.5.2.2 Łączenie do sieci bezprzewodowej klientów Windows

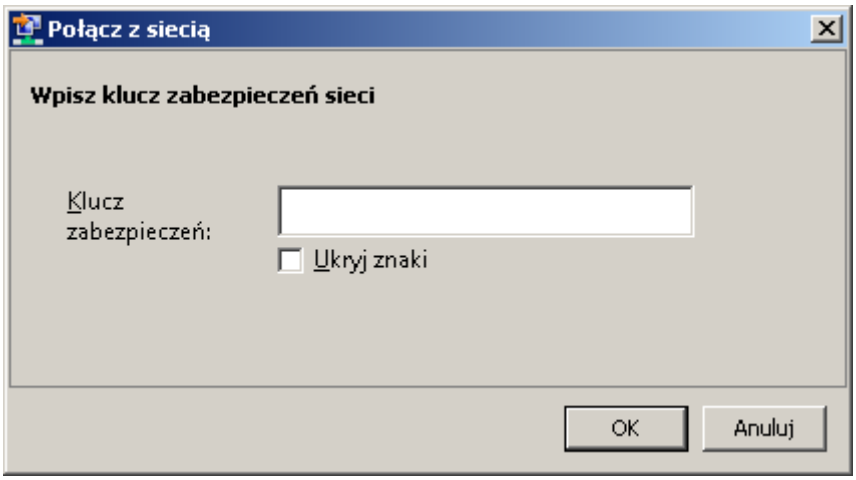
Jeśli komputer posiada funkcje bezprzewodowe (kartę bezprzewodową) Microsoft Windows ™ automatycznie rozpozna i wyświetli ikonę połączenia bezprzewodowego w zasobniku systemowym (alternatywnie, ta ikona jest wyświetlana w Windows XP „Połączenia sieciowe" → Windows 7 „Centrum sieci i udostępniania". Kliknij ikonę, aby wyszukać i połączyć się z siecią bezprzewodową bramy. Alternatywnie można skorzystać z bezprzewodowego oprogramowania klienckiego dostarczonego do urządzenia bezprzewodowego, aby podłączyć się do sieci bezprzewodowej.

Aby ręcznie nawiązać połączenie bezprzewodowe między komputerem a bramą, wykonaj następujące polecenie:

1. Kliknij dwukrotnie na ikonę połączenia bezprzewodowego, które pojawia się w zasobniku systemowym. Ekran połączenie sieciowe, wyświetla bezprzewodowe połączenie OpenRG. Należy pamiętać, że połączenie jest zdefiniowane jako połączenie z zabezpieczeniami sieci bezprzewodowej (WPA).

Rysunek 6.51 Dostępne sieci bezprzewodowe

2. Kliknij na wybrane połączenie raz, aby go zaznaczyć, a następnie kliknij przycisk „Połącz". Poniżej pojawia się okno logowania z prośbą o klucz sieciowy, który jest kluczem wstępnym i został skonfigurowany wcześniej na naszym urządzeniu.

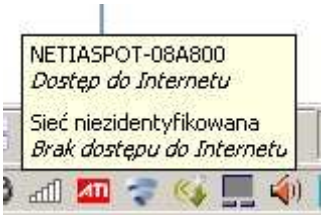


Rysunek 6.52 Łączenie się do zabezpieczonej sieci bezprzewodowej

3. Wprowadź klucz wstępny w obu polach i kliknij przycisk „OK". Po połączeniu do sieci bezprzewodowej, jej stan zmieni się na „Połączony".

Rysunek 6.53 Połączenie z siecią bezprzewodową

Dymek jest wyświetlany w obszarze powiadomień, oznaczając powodzenie i podłączenie do sieci bezprzewodowej.

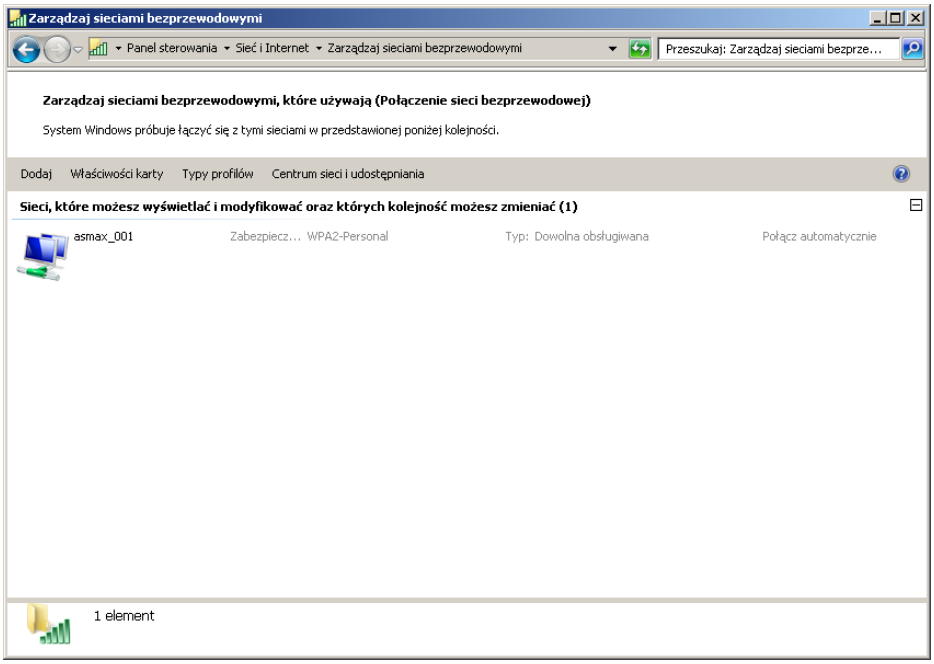


Rysunek 6.54 Informacje o połączeniu bezprzewodowym

4. Przetestuj połączenie poprzez odłączenie wszystkich innych sieci i przeglądaj Internet za pomocą połączenia bezprzewodowego.

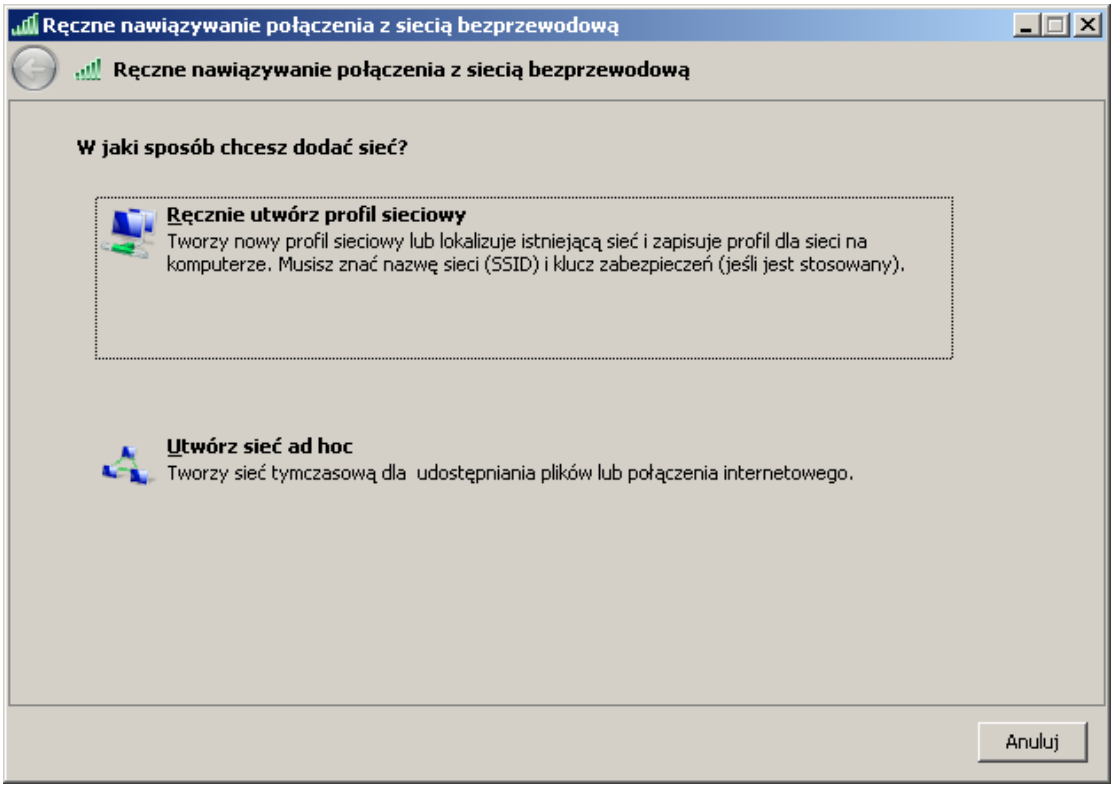
Jeśli okno logowania nie pojawi się powyżej i próba połączenia zakończy się niepowodzeniem, należy skonfigurować bezprzewodowe połączenie ręcznie:

1. Kliknij raz na połączenie, aby go zaznaczyć, a następnie kliknij link „Centrum sieci i udostępniania”, następnie na „Zarządzaj sieciami bezprzewodowymi”, w polu „Sieci, które możesz wyświetlać i modyfikować…”. Wpisy, które są tam zamieszczone do już istniejące profile sieci bezprzewodowych, możemy dodać nowe lub skasować stare (patrz rys. 6.51).

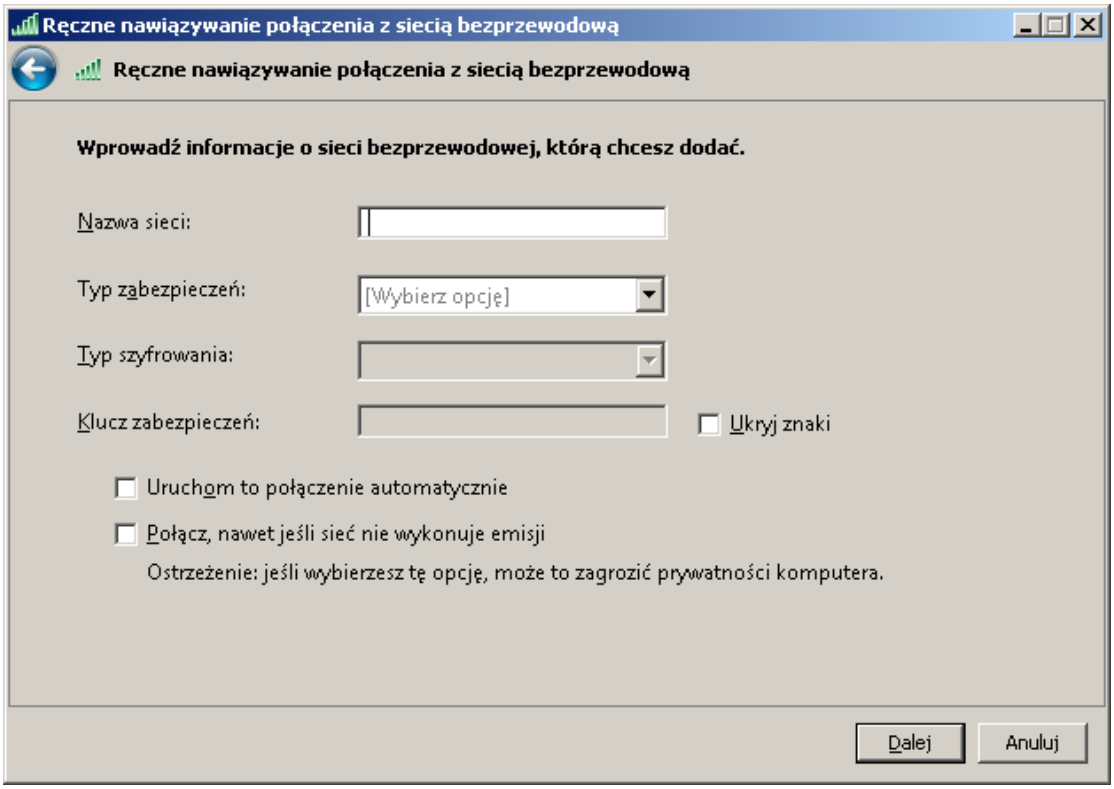


Rysunek 6.55 Panel sterowania - Centrum sieci i udostępniania – Zarządzaj sieciami bezprzewodowymi

2. Wybierz opcję „Dodaj”(patrz rysunek 6.55). Wyświetlone zostanie poniższe okno dialogowe, gdzie wybierzemy „Ręcznie utwórz profil sieciowy”.



3. Kliknij „Ręcznie utwórz profil sieciowy”, a następnie uzupełnij pola o odpowiednie dane. Wyświetlone zostanie okno, jak poniżej.



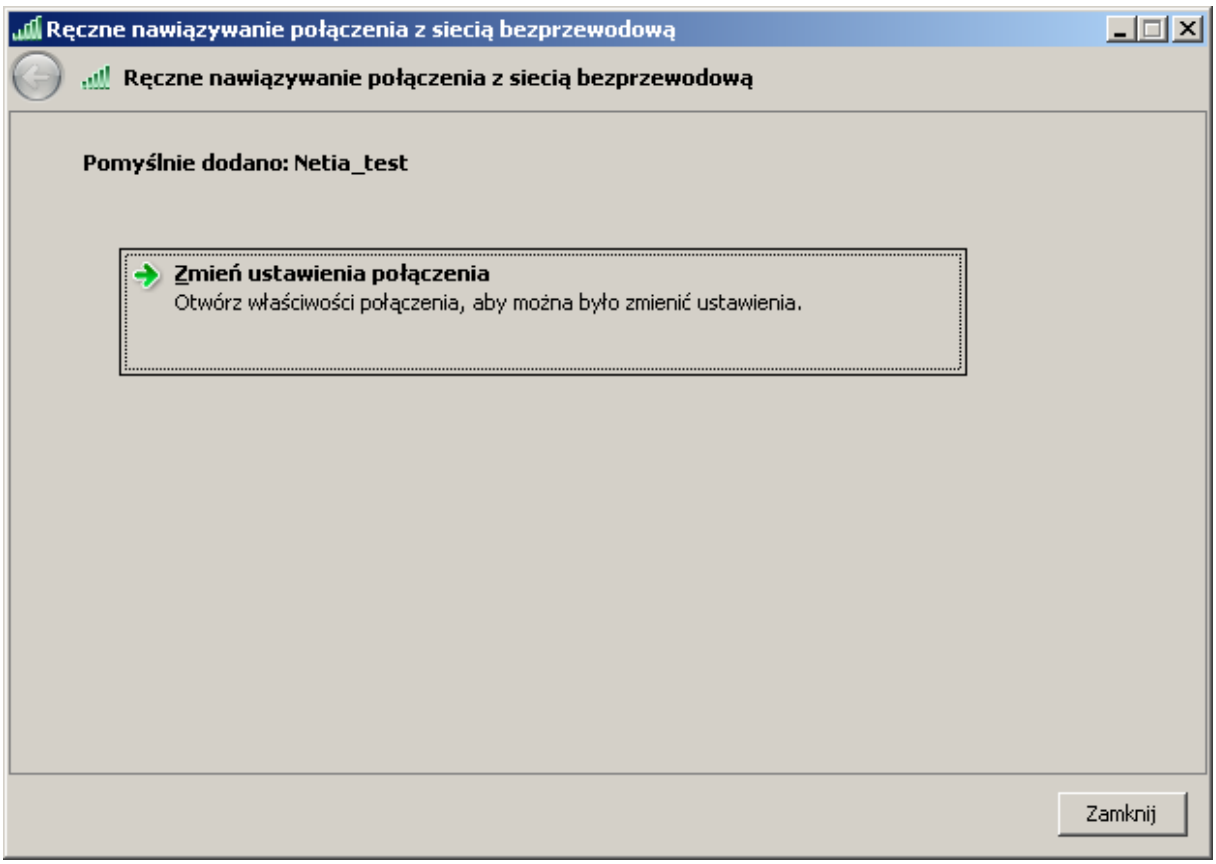
a. Z menu rozwijanego menu „Typ zabezpieczeń” wybierz „WPA Personal”.

b. Z rozwijanego menu wybierz „Szyfrowanie danych”, wybierz „TKIP”.

c. Wpisz swój klucz zabezpieczeń jako „Klucz zabezpieczeń” i „Potwierdź klucz sieciowy”.

4. Kliknij przycisk „Dalej” w obu oknach, aby zapisać ustawienia.

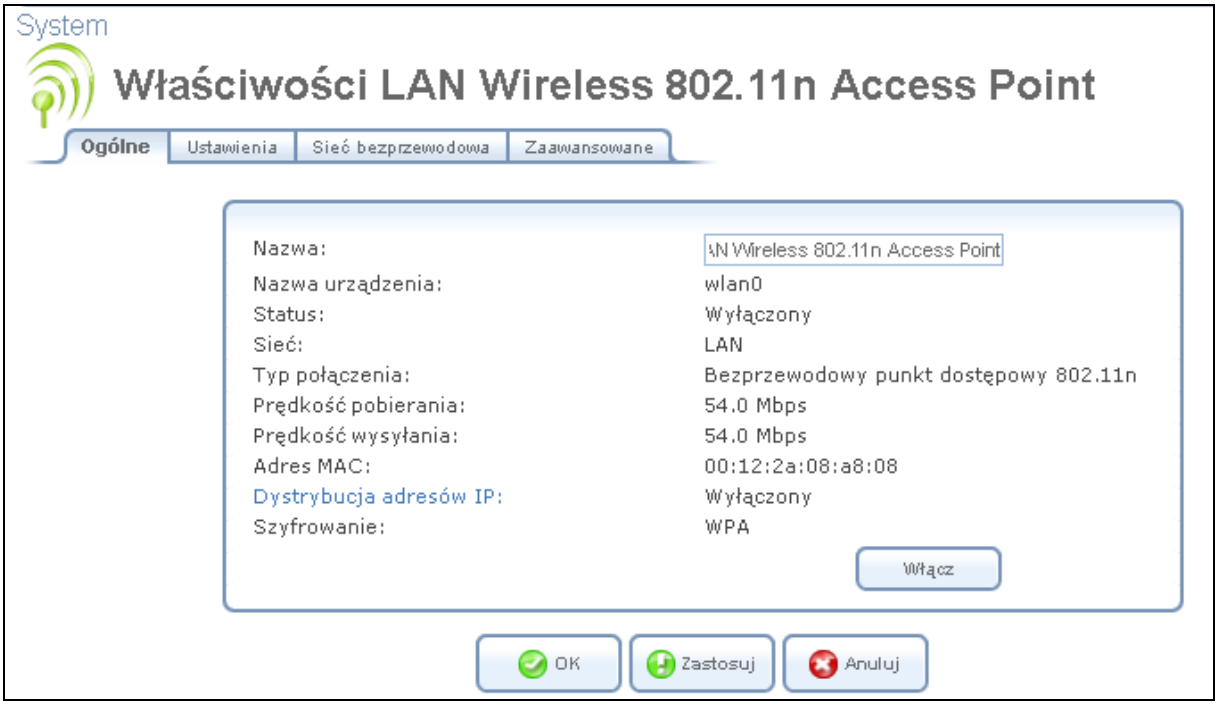
5. Po dodaniu ręcznie profilu sieci bezprzewodowej, wyświetlone zostanie okno jak poniżej.



Ponieważ sieć jest zabezpieczona tylko użytkownicy, którzy znają klucza zabezpieczeń będą mogli się połączyć. Należy pamiętać, że przy wyborze WPA, WPA i WPA2 są obsługiwane.

6.4.5.3 Konfiguracja ogólnych parametrów sieci bezprzewodowej.

Sekcja „Właściwości Wireless LAN Access Point 802.11n" wyświetla szczegółowe podsumowanie dotyczące parametrów bezprzewodowego połączenia.



Rysunek 6.57 Właściwości połączenia wbudowanego bezprzewodowego punktu dostępowego

Użyj zakładki „Ustawienia" w celu edycji parametrów.

Ogólne - ta sekcja wyświetla ogólne parametry połączenia bezprzewodowego. Zaleca się nie zmieniać wartości domyślnych, chyba że jesteśmy zaznajomieni z pojęciami sieciowymi zawartymi w sekcji. Ponieważ brama jest skonfigurowana do pracy z wartościami domyślnymi, nie jest konieczne wprowadzenie modyfikacji parametrów.

Rysunek 6.58 Ustawienia parametrów sieci bezprzewodowej

Harmonogram - domyślnie połączenie jest zawsze aktywne. Jednakże, można skonfigurować zasady harmonogramu w celu określenia segmentów czasu, w którym połączenie może być aktywne. Po wybraniu zdefiniowanej reguły, z rozwijanego menu pozwala na wybór pomiędzy dostępnymi regułami. Aby dowiedzieć się, jak skonfigurować reguły harmonogramu, możemy odnieść się do „Definiowania reguł harmonogramu" w części administracyjnej instrukcji OpenRG.

Sieć - wybierz, czy parametry konfigurowane odnoszą się do połączenia WAN, LAN lub DMZ wybierając typ połączenia z rozwijanego menu. Aby uzyskać więcej informacji, odnoszących się do powyższej funkcji, możemy ich znaleźć w sekcji „Typy sieci" administracyjnej instrukcji OpenRG. Należy pamiętać, że przy definiowaniu połączenia sieci jako DMZ, należy także:

• Odłączyć połączenie z mostu, jeśli takie istnieje.
• Zmiana trybu połączenia trasy do „Route", w „Routingu".
• Dodaj reguły routingu na zewnątrz bramy (które mogą być dostarczane przez ISP), informuj sieć DMZ za OpenRG.

Adres fizyczny - adres fizyczny interfejsu sieciowego w sieci. Niektóre interfejsy pozwalają na zmianę tego parametru.

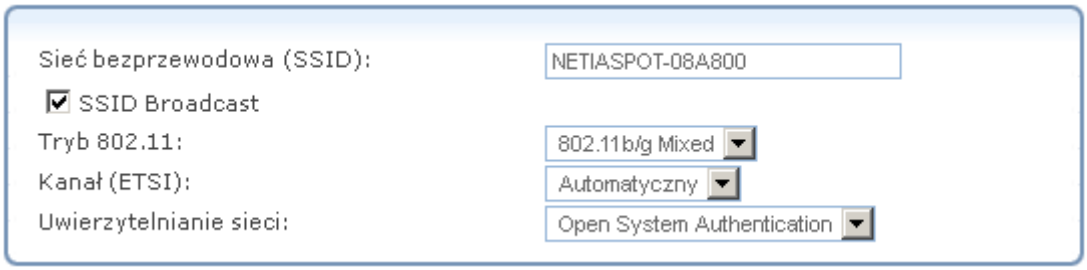
MTU - MTU jest to maksymalna jednostka transmisji. Określa ona największy rozmiar pakietu, jakim możemy przekazywać dane do Internetu. W ustawieniach domyślnych, automatycznie brama wybiera najlepsze MTU dla połączenia internetowego. Wybierz opcję „Automatycznie przez serwer DHCP", wtedy DHCP określenia wielkość MTU. W przypadku wybrania opcji „Ręcznie" zaleca się wpisać wartość od 1200 do 1500.

6.4.5.4. Definiowanie zaawansowanych ustawień bezprzewodowego punktu dostępowego

Sekcja ustawień „Sieć bezprzewodowa" i zakładka „Zaawansowane" umożliwiają wykonywanie zaawansowanych konfiguracji bezprzewodowego punktu dostępu.

6.4.5.4.1. Sieć bezprzewodowa

W tej sekcji określono podstawowe ustawienia bezprzewodowego punktu dostępu.



Rysunek 6.59 Bezprzewodowy punkt dostępowy

SSID Broadcast (rozgłaszanie) - domyślnie OpenRG transmituje nazwę sieci bezprzewodowej (SSID). Ze względów bezpieczeństwa, można ukryć w sieci bezprzewodowej rozgłaszanie nazwy sieci naszego urządzenia poprzez odznaczenie tej opcji. Klienci łączący się do naszej sieci bezprzewodowej będą mogli łączyć się przez ręczne wpisanie SSID w aplikacji klienckich karty bezprzewodowej (Windows lub aplikacji innej firmy), a nie wybierając, jak wcześniej nazwę sieci bezprzewodowej z listy dostępnych sieci bezprzewodowych.

Tryb 802.11 - wybierz żądany typ połączenia bezprzewodowego. Domyślnie jest ustawiony na 802.11g/n. Należy pamiętać, że starsze urządzenia 802.11b nie są zgodne z trybem 802.11g/n oraz samym 802.11g.

Kanał - wszystkie urządzenia w sieci bezprzewodowej sieci nadają na różnych kanałach. Pozostawianie tego parametru jako „Automatyczny" zapewnia sprawdzanie na bieżąco przez OpenRG dostępnych kanałów w sieci bezprzewodowej na danym obszarze. Możliwe

jest też, aby wybrać kanał ręcznie, jeśli posiadamy informacje dotyczące kanałów bezprzewodowy używanych, w naszym otoczeniu.

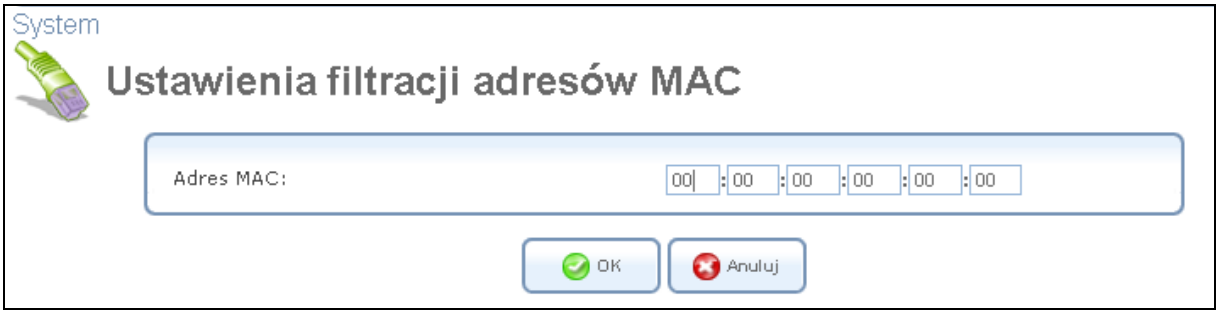
Tryb szerokości kanału – wybierz szerokości kanału dla sieci bezprzewodowej, w zależności od wybranego standardu komunikacji. Dla „b" oraz „g", wybierz opcję „Tylko 20 MHz" lub „20/40 MHz (dynamiczny)". W trybie 802.11n mogą być wybrane dowolne ustawienia.

Uwierzytelnianie sieci - metoda uwierzytelnienia WPA „Open System Authentication" oznacza, że klucz sieciowy nie jest używany do uwierzytelniania. Używając protokołów zabezpieczeń 802.1X WEP lub Non-802.1X WEP, możemy zmienić i wybrać z rozwijanego menu metodę „Shared Key Authentication" (która korzysta ze współdzielonego klucza sieciowego do uwierzytelniania) lub możemy wybrać obie metody łącznie.

MAC Filtering – można filtrować klientów bezprzewodowych w zależności od ich adresu MAC, zezwalać lub odmawiając im dostępu do sieci bezprzewodowej. Aby dodać regułę filtrowania MAC, należy wybrać akcję do wykonania w rozwijanym menu. Następnie kliknij przycisk „Nowy adres MAC". Ekran ustawień filtracji adresów MAC jest widoczny poniżej.

6.4.5.4.2 Tabela filtracji adresów MAC

W tej sekcji określamy zaawansowane ustawienia punktu dostępu bezprzewodowego. Kliknij przycisk „Nowy adres MAC", aby zdefiniować filtrowanie adresów MAC. Wyświetlony zostanie ekran ustawień filtracji adresów MAC.



Rysunek 6.60 Ustawienia filtracji adresów MAC

Wpisz adres MAC do filtrowania i kliknij przycisk „OK”. Lista adresów MAC wyświetlona zostanie w wybranych akcjach filtrowania (zezwalaj/odrzuć) i zostanie wykonana.

Rysunek 6.61 Tabela filtracji adresów MAC

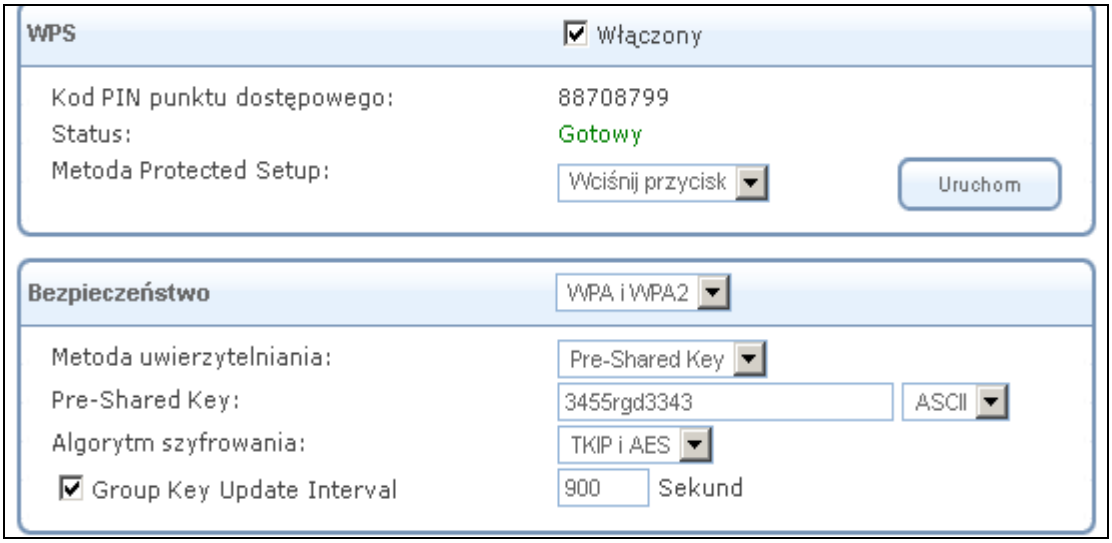
6.4.5.4.3 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) jest sposobem na uproszczenie instalacji bezpieczeństwa i zarządzania siecią bezprzewodową. Ta funkcja jest dostępna w OpenRG, ale jest domyślnie wyłączona. Po włączeniu można kontrolować konfigurację zabezpieczeń sieci bezprzewodowej, która jest określona w poniższej sekcji „Bezpieczeństwo" (patrz punkt 6.4.5.4.4). Należy pamiętać, że tylko WPS obsługuje protokół zabezpieczeń WPA, dlatego po włączeniu tej funkcji, wszystkie inne rodzaje i protokoły są wyłączone (nie będą już dostępne w dziale „Bezpieczeństwo” w rozwijanym menu). Aby włączyć WPS, kliknij „Włączony” w polu wyboru. Ekran zostanie odświeżony.

Aby włączyć WPS, kliknij "Włączony" w polu wyboru. Ekran odświeży zawartość sekcji.

Rysunek 6.62 Wi-Fi Protected Setup

Utwórz klucz automatycznie - możesz wprowadzić klucz zabezpieczeń ręcznie, lub zlecić jego generowane automatycznie. Wybierz swoje preferencje, używając pola wyboru i kliknij przycisk „Zastosuj". Ekran zostanie odświeżony.



Rysunek 6.63 Włączona funkcja WPS

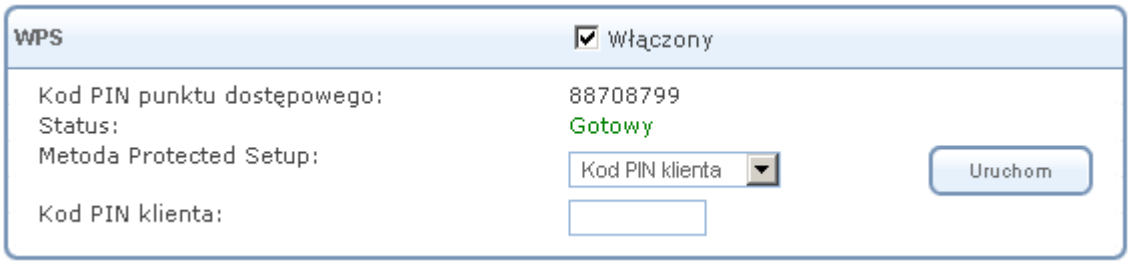
Jeśli wybrano automatyczne generowanie klucza, klucz wstępny (wartości szesnastkowe) został wygenerowany, pojawi się w sekcji „Bezpieczeństwo". Można wprowadzić/zmienić wartość klucza w każdej chwili wpisując inny w tej sekcji, jak również zmienić typ wartości na ASCII używając rozwijanego menu.

Status - określa stan WPS. Status oznaczony jako „Gotowy" oznacza, że system jest gotowy do negocjacji przychodzących od klientów bezprzewodowych, lub „rejestrujących".

Metoda Protected Setup - OpenRG obsługuje dwie metody połączenia „Push Buton" (metoda domyślna) i „PIN kod klienta". Są to metody stosowane przez klientów bezprzewodowych w poszukiwaniu punktu dostępu wspierającego WPS.

• **Push Buton** (naciśnij przycisk) - rejestracja jest inicjowana przez fizyczne wciśnięcie przycisku na karcie bezprzewodowej klienta lub poprzez oprogramowanie. Po rozpoczęciu rejestracji, kliknij przycisk „Uruchom" lub naciśnij przycisk WPS znajdujący się na tyle urządzenia, aby twoje urządzenie oczekiwało na połączenie ze stacji klienckiej.

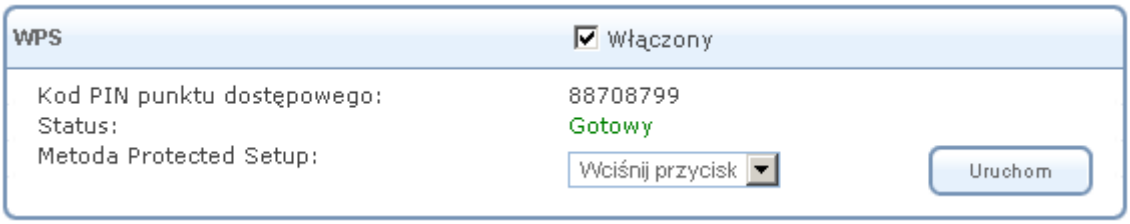
• **Kod PIN klienta** - rejestracja jest inicjowana przez oprogramowanie klienta bezprzewodowego, które musi wspierać metodę kodu PIN. Aby uzyskać połączenie w ten sposób, należy wybrać tę opcję z menu rozwijanego. Zostanie wyświetlone pole do wprowadzenia kodu PIN.



Rysunek 6.64 Metoda automatycznej konfiguracji zabezpieczeń – Kod PIN

W tym polu wprowadź czterocyfrowy kod PIN dostarczony przez oprogramowanie klienta bezprzewodowego. Kliknij przycisk „Uruchom" w urządzeniu, aby nawiązać połączenie.

Przed podłączeniem klienta sieci bezprzewodowej do sieci bezprzewodowej OpenRG przy wykorzystaniu WPS, musimy wiedzieć, z jakiej metody automatycznej konfiguracji będziemy korzystać. Po wciśnięciu przycisku WPS nasze urządzenie będzie czekać dwie minuty na klienta chcącego uzyskać połączenie. Gdy połączenie zostanie ustanowione, pole „Status" zmieni status, aby o tym poinformować.



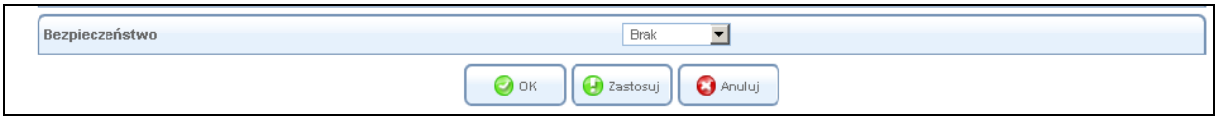
Rysunek 6.65 Status funkcji WPS

Należy pamiętać, że funkcja WPS jest obsługiwana tylko z zabezpieczeniem WPA. Dlatego też, gdy korzystamy z „WEP" lub sieci niezabezpieczonej, wybranych z rozwijanego menu „Zabezpieczenia", pojawi się poniższy komunikat w sekcji WPS.

6.4.5.4.4 Bezpieczeństwo sieci bezprzewodowej

Sekcja, pozwala aby skonfigurować ustawienia zabezpieczeń sieci bezprzewodowej. Wybierz typ zabezpieczeń protokołu z rozwijanego menu „Typ zabezpieczenia". Po odświeżeniu ekranu, przedstawiony zostanie odpowiednio każdy protokół konfiguracji.

• **Brak** - wybranie tej opcji wyłącza zabezpieczenia połączenia bezprzewodowego. Każdy bezprzewodowy komputer w danym obszarze będą w stanie połączyć się z internetem przy użyciu naszego połączenia **(opcja nie jest zalecana).**



Rysunek 6.66 Wyłączone zabezpieczenia sieci bezprzewodowej

• **WPA** jest metodą szyfrowania danych w standardzie 802.11 w bezprzewodowej sieci LAN (patrz punkt 6.4.5.2).

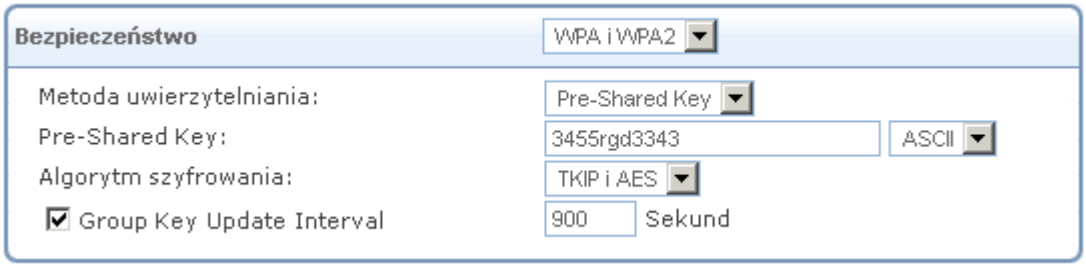
Metoda uwierzytelniania Wybierz metodę uwierzytelniania jakiej chcesz użyć. Można wybrać Pre-Shared Key i 802.1x.

Pre-Shared Key - Ten wpis pojawia się tylko w przypadku wybrania tej metody uwierzytelniania. Wprowadź klucz szyfrowania w polu „Pre-Shared Key". Możesz użyć ASCII lub wartości Hex, wybierając typ wartość w menu rozwijanym.

Algorytm szyfrowania - wybierz między algorytmami szyfrowania „Temporal Key Integrity Protocol" (TKIP) i „Advanced Encryption Standard" (AES) .

Group Key Update Interval - definiuje okres czasu aktualizacji grupy klucz w sekundach.

Inter Client Privacy (izolacja klientów sieci bezprzewodowej) - zaznacz pole wyboru, aby zapobiec komunikacji między klientami w sieci bezprzewodowej przy użyciu tego samego punktu dostępu. Klienci nie będą mogli przeglądać i mieć dostępu do siebie nawzajem podobnie jak do udostępnionych katalogów.



Rysunek 6.67 Parametry WPA

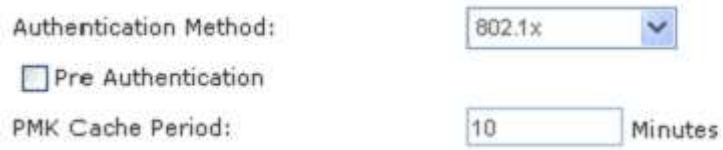
• WPA2 - to udoskonalona wersja WPA i definicji protokołu 802.11i.

Metoda uwierzytelniania - wybierz metodę uwierzytelniania jaką chcesz użyć. Można wybrać Pre-Shared Key i 802.1x.

Pre-Shared Key - ten wpis pojawia się tylko w przypadku wybrania tej metody uwierzytelniania. Wprowadź klucz szyfrowania w polu „Pre-Shared Key". Możesz użyć ASCII lub wartości Hex, wybierając typ wartości w rozwijanym menu.

Pre Authentication – przy wyborze metody uwierzytelniania 802.1x, te dwa wpisy pojawiają się (patrz rysunek 6.68). Wybierz tę opcję, aby umożliwić OpenRG współpracę z serwerem RADIUS i przesyłać żądania uwierzytelnienia z komputerów podłączonych do innych punktów dostępu. Dzięki temu jest możliwy roaming z jednej sieci bezprzewodowej do innej.

PMK Cache Period - liczba minut przed usunięciem (i wznowieniem) z „Pairwise Master Key", służy do uwierzytelniania.

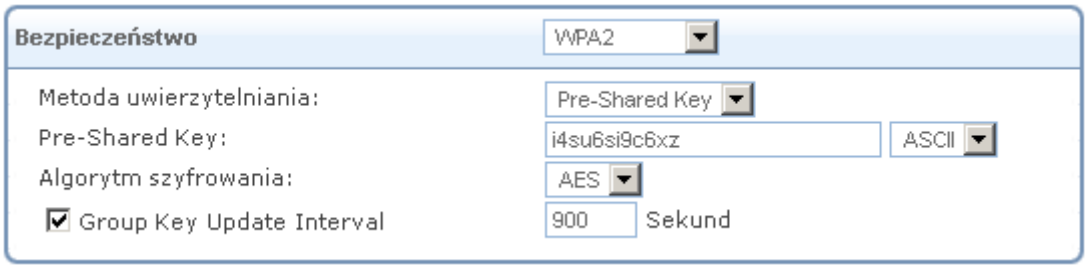


Rysunek 6.68 Metoda uwierzytelniania 802.1x

Algorytm szyfrowania - algorytmu szyfrowania WPA2 jest używany do zaawansowanego szyfrowania z użyciem protokołu AES.

Group Key Update Interval - definiuje okres czasu aktualizacji grupy kluczy w sekundach.

Inter Client Privacy (izolacja klientów sieci bezprzewodowej) - zaznacz pole wyboru, aby zapobiec komunikacji między klientami w sieci bezprzewodowej przy użyciu tego samego punktu dostępu. Klienci nie będą mogli przeglądać i mieć dostępu do siebie nawzajem podobnie jak do udostępnionych katalogów.



Rysunek 6.69 Parametry WPA2

• **WPA i WPA2 Tryb mieszany** - WPA i WPA2 są to zróżnicowane metody szyfrowania danych.

Metoda uwierzytelniania - wybierz metodę uwierzytelniania, którą chcesz użyć. Można wybrać Pre-Shared Key i 802.1x.

Pre-Shared Key - ten wpis pojawia się tylko w przypadku wybrania tej metody uwierzytelniania. Wprowadź klucz szyfrowania w polu „Pre-Shared Key". Możesz użyć ASCII lub wartości Hex, wybierając typ wartość z rozwijanego menu.

Pre Authentication – przy wyborze metody uwierzytelniania 802.1x, te dwa wpisy pojawiają się (patrz rysunek 6.68). Wybierz tę opcję, aby umożliwić OpenRG współpracę z serwerem RADIUS i przesyłać żądania uwierzytelnienia z komputerów podłączonych do innych punktów dostępu. Dzięki temu jest możliwy roaming z jednej sieci bezprzewodowej do innej.

PMK Cache Period - liczba minut przed usunięciem (i wznowieniem) z „Pairwise Master Key", służy do uwierzytelniania.

Rysunek 6.70 Metoda uwierzytelniania 802.1x

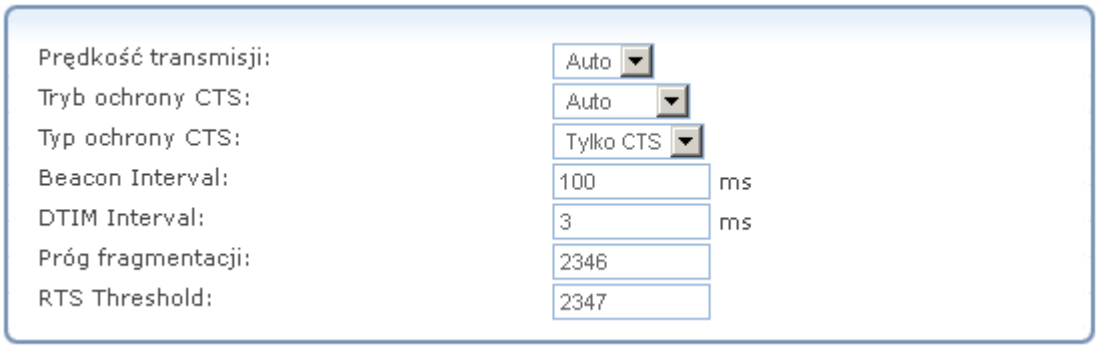
Algorytm szyfrowania - algorytmu szyfrowania WPA2 jest używany do zaawansowanego szyfrowania z użyciem protokołu AES.

Group Key Update Interval - definiuje okres czasu aktualizacji grupy kluczy w sekundach.

Inter Client Privacy (izolacja klientów sieci bezprzewodowej) - zaznacz pole wyboru, aby zapobiec komunikacji między klientami w sieci bezprzewodowej przy użyciu tego samego punktu dostępu. Klienci nie będą mogli przeglądać i mieć dostępu do siebie nawzajem podobnie jak do udostępnionych katalogów.

6.4.5.4.5 Właściwości transmisji bezprzewodowej

W tej sekcji zostaną opisane właściwości transmisji bezprzewodowej.



Rysunek 6.82 Właściwości transmisji

Prędkość transmisji - szybkość transmisji jest ustawiona w zależności od prędkości sieci bezprzewodowej połączenia. Wybierz szybkość transmisji z rozwijanego menu lub wybierz opcję „Auto, aby OpenRG automatycznie pracowało z największą możliwą szybkością transmisji danych (opcja dostępna tylko przy 802.11ng). Należy pamiętać, że jeśli

połączenie bezprzewodowe jest słabe lub niestabilny, najlepiej jest wybrać niską szybkości transmisji.

Moc nadajnika - procent maksymalnej mocy nadawania.

Tryb ochrony CTS - zwiększa zdolność bramy do przechwytywania transmisji 802.11g oraz 802.11b. Natomiast „tryb ochrony CTS" zmniejsza wydajność. Pozostaw domyślne parametry tej funkcji, chyba że wystąpią poważne trudności w komunikacji między bramą OpenRG i 802.11g –wtedy wybierzemy opcję „Zawsze". Domyślną opcją jest „Auto", aby OpenRG automatycznie podejmowało decyzję, czy korzystać z tej funkcji.

Typ ochrony CTS - wybierz typ CTS ochrony „Tylko CTS" lub „RTS-CTS".

Beacon Interwal (Czas pomiędzy sygnałami identyfikacji) - znacznik jest to pakiet nadany przez OpenRG do synchronizacji sieci bezprzewodowej. Wartość odstępu wskazuje, jak często beacon jest wysyłany do każdego bezprzewodowego komputera klienckiego/punktu dostępu, pakiet wysyłany w celu poinformowania o danej aktywności w sieci. Zalecane jest pozostawienie wartości domyślnych.

DTIM Interval - (Częstotliwość pakietów DTIM) Delivery Traffic Indication Message (DTIM), informuje klientów bezprzewodowych o następnej możliwość otrzymania pakietu multicast i broadcast. Wartość ta waha się pomiędzy 1 i 16384. DTIM to wiadomość rozsyłana do komputerów klienckich, które posiadają obsługę zarządzania energią, DTIM przesyła informacje o pojawieniu się danych, które mają zostać do nich przesłane. Jest to informacja dla klienckiego urządzenia, że musi przejść w tryb aktywności, aby otrzymać dane. Mniejsza wartość DTIM będzie skutkować, że podłączony klient nie będzie długo pracował w trybie oszczędzania energii. Większa wartość oznacza, że klient może przejść w tryb oszczędzania energii i jednocześnie dłużej pracować w trybie aktywności, ze względu na przesyłanie większej ilości danych. Zalecane jest pozostawienie domyślnej wartości.

Próg fragmentacji pakietów – pakiety, które są większe niż określony próg, są podzielone na kilka mniejszych pakietów. Spróbuj zwiększyć próg fragmentacji w przypadku napotkania dużej ilości błędów w transmisji (większość problemów z transmisją pojawia się dlatego, że w otoczeniu naszego punktu dostępowego istnieje inny ruch i transmisje bezprzewodowe kolidują ze sobą). Nie ustawiaj zbyt małej wartości, ponieważ może to doprowadzić do ograniczenia wydajności sieci bezprzewodowej. Zalecane jest pozostawienie wartości domyślnych.

RTS Threshold - (Próg dla żądania wysłania) – jest to czas, który OpenRG odczekuje przed wysłaniem wiadomości RTS do komputera klienckiego. Pakiet RTS informuje, że klient będzie wysłał dane i potrzebuje uprzywilejowanego dostępu przez czas trwania transmisji i odbierania danych. Klient bezprzewodowy odpowiada pakietem „Clear to Send" (CTS), sygnalizując, że transmisja może się rozpocząć. W przypadku pakietów mniejszych niż ustalony próg RTC/CTS mechanizm nie jest aktywny. Jeśli napotkasz niespójne dane transmisji, spróbuj zmniejszyć próg RTS. Zalecane jest pozostawienie wartości domyślnych.

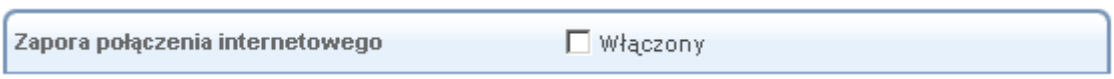
6.4.5.4.6 Wirtualne punkty dostępowe

Możesz ustawić wiele wirtualnych sieci WLAN na OpenRG, ograniczenia są tylko co do liczby obsługiwanej przez moduł bezprzewodowy. Takie wirtualne sieci WLAN są określane jako „Wirtualny punkt dostępu".

6.4.5.4.7 Zaawansowane

Użyj sekcji „Zaawansowane", aby skonfigurować następujące parametry:

• Zapora połączenia internetowego - zapora sieciowa naszego urządzenia pomaga chronić komputery w sieci i zapobiega przed nieautoryzowanym uzyskaniem dostępu do niego za pośrednictwem sieci, takiej jak Internet. Zapora może być aktywowana na wybranym połączeniu z siecią. Aby włączyć funkcje zapory w połączeniu sieciowym, wybierz pole wyboru „Włączony". Aby dowiedzieć się więcej na temat zabezpieczeń, patrz punkt 5.2.



Rysunek 6.90 Zapora połączenia internetowego

• **Dodatkowe adresy IP** - można dodać aliasy (dodatkowe adresy IP) bramy, klikając link „Nowy adres IP". Pozwala to na dostępu do bramy za pomocą aliasów oprócz domyślnych 192.168.1.254 i http://netiaspot.home.

Rysunek 6.91 Dodatkowe adresy IP

6.4.6. Konfigurowanie połączenia Ethernet WAN

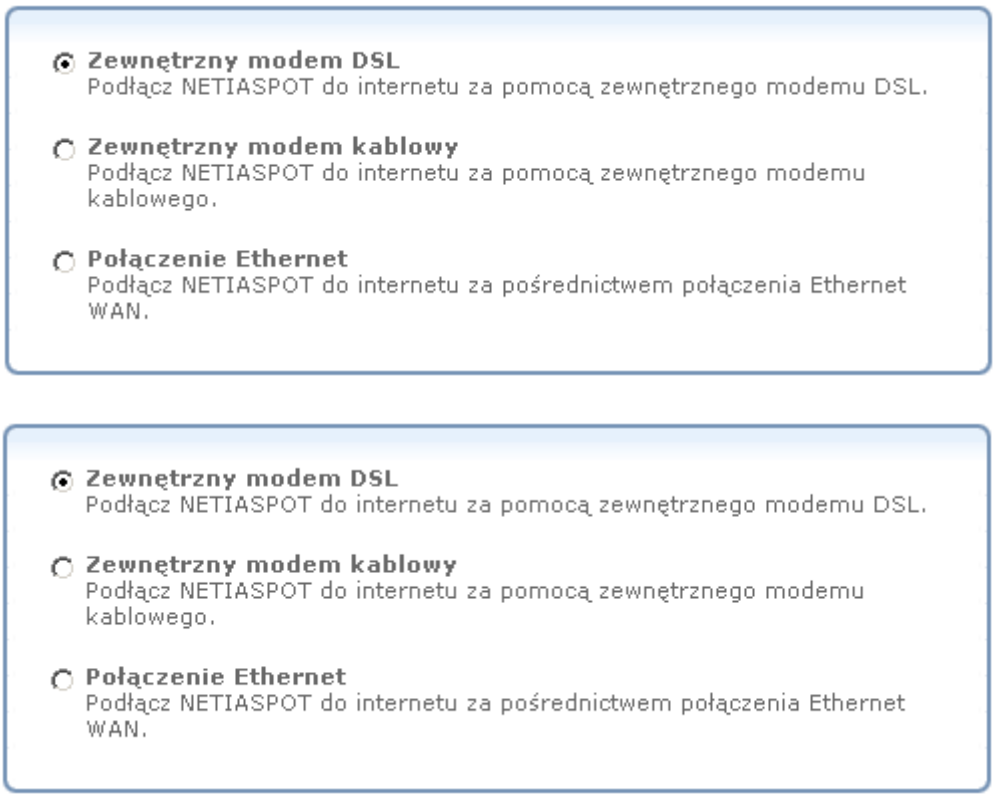
Połączenie Ethernet WAN umożliwia podłączenie OpenRG do innej sieci albo bezpośrednio lub przez modem zewnętrzny. Kreator połączeń zawiera szereg metod szybkiego utworzenia takiego połączenia.

6.4.6.1. Korzystanie z kreatora połączeń Ethernet

Narzędzie kreatora połączeń Ethernet jest najbardziej podstawową metoda konfigurowania połączenia WAN Ethernet. Metoda ta przeznaczona jest dla połączeń, które nie wymagają nazwy użytkownika i hasła, aby połączyć się z internetem.

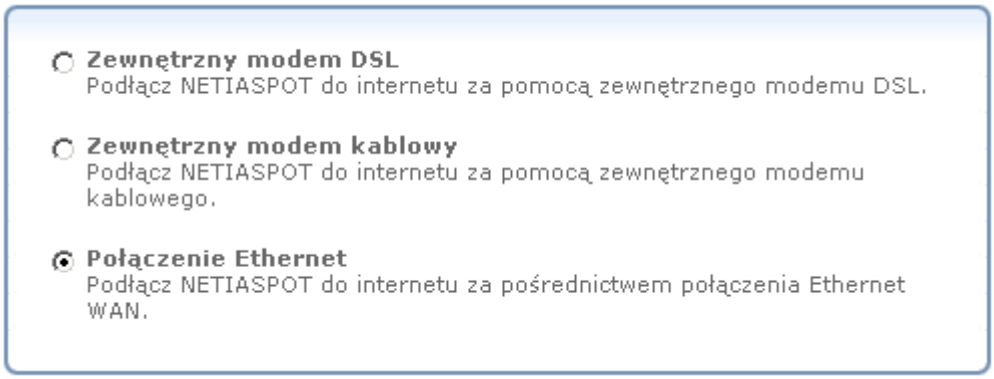
Aby utworzyć nowe połączenie Ethernet, wykonaj następujące czynności:

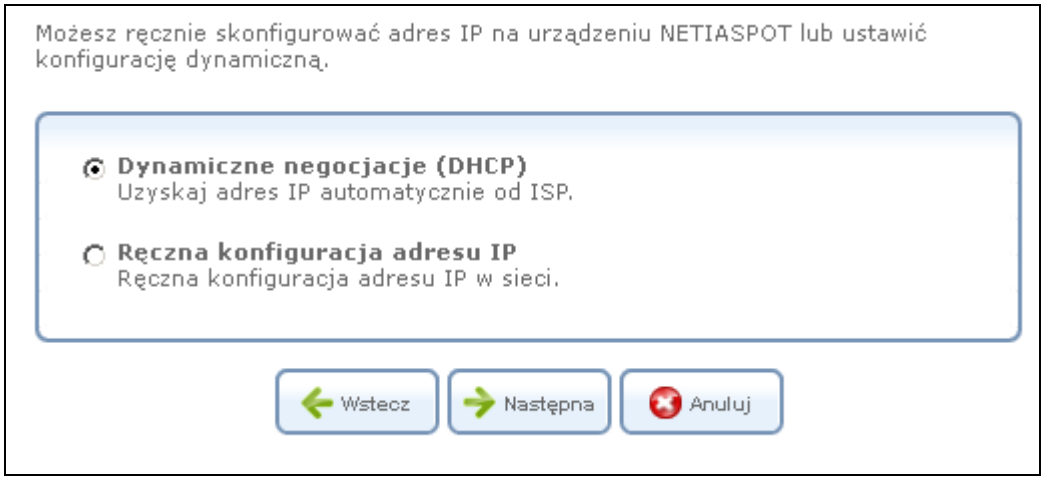
1. Kliknij przycisk „Nowe połączenie" w menu „Połączenia sieciowe" (patrz Rysunek 6.10). Zostanie wyświetlony ekran „Kreator połączeń" (patrz rysunek 6.18).
2. Wybierz opcję „Połączenie internetowe", a następnie przycisk „Dalej". Wyświetlony zostanie ekran „Połączenie internetowe" (patrz rysunek 6.19).
3. Wybierz przycisk „Zewnętrzny modem kablowy", a następnie przycisk „Dalej".



Rysunek 6.92 Połączenie z Internetem za pomocą zewnętrznego modemu kablowego

4. Wybierz „Połączenie Ethernet”, a następnie przycisk „Dalej”. Wyświetlony zostanie ekran „Podsumowanie połączenia”.





Rysunek 6.93 Podsumowanie połączenia

5. Wybierz pole wyboru „Edytuj nowo utworzone połączenie", jeśli chcesz nie chcesz przechodzić do ekranu edycji połączenia, kliknij „Koniec". Ekran ten jest opisany w dalszej części tego rozdziału.
6. Kliknij przycisk „Koniec", aby zapisać ustawienia.

Połączenie Ethernet WAN zostanie odpowiednio skonfigurowane. Patrz sekcja 6.4.6.4, aby dowiedz się, jak przeglądać i edytować ustawienia połączenia.

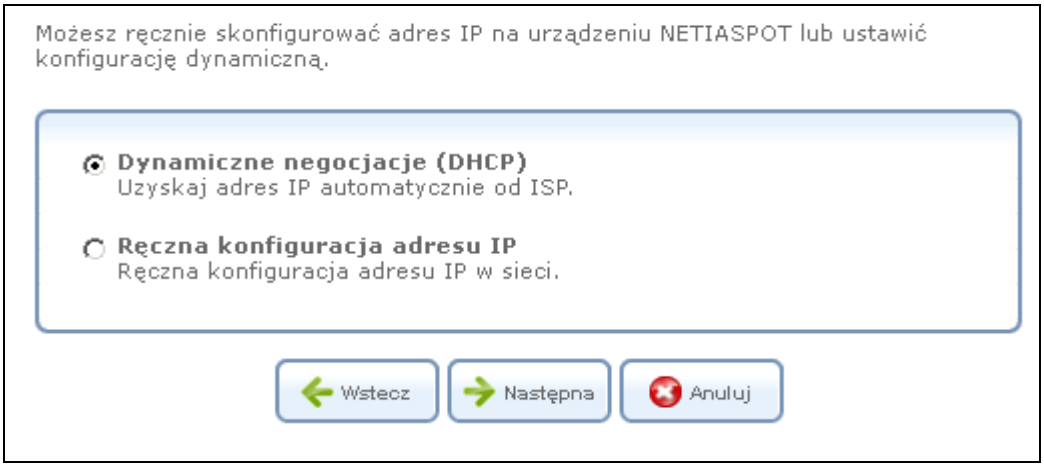
6.4.6.2 Korzystanie z kreatora połączeń Ethernet z użyciem DHCP

Dynamic Host Configuration Protocol (DHCP) narzędzie kreatora połączenia do dynamicznej

metody negocjacji nawiązywania połączenia Ethernet WAN. Korzystając z tej metody, klient otrzymuje adres IP automatycznie od usługodawcy podczas łączenia się z Internetem.

Aby utworzyć nowe połączenie WAN DHCP oparte na połączeniu Ethernet, wykonaj następujące czynności:

1. Kliknij przycisk „Nowe połączenie" w sekcji „Połączenia sieciowe" (patrz Rysunek 6.10). Wyświetlony zostanie ekran „Kreator połączenia" (patrz rysunek 6.18).
2. Wybierz opcję „Połączenie z Internetem DSL", a następnie przycisk „Dalej"(patrz rysunek 6.19).
3. Wybierz „Połączenie Ethernet", a następnie przycisk „Dalej".



Rysunek 6.94 Połączenie Ethernet

4. Wybierz opcję „Dynamiczne negocjacje (DHCP)", a następnie przycisk „Dalej". Wyświetlony zostanie ekran podsumowujący połączenie.

Rysunek 6.95 Podsumowanie połączenia

5. Wybierz pole wyboru „Edytuj nowo utworzone połączenie", jeśli nie chcesz przechodzić do ekranu edycji połączenia, kliknij „Koniec". Ekran ten jest opisany w dalszej części tego rozdziału.
6. Kliknij przycisk „Koniec", aby zapisać ustawienia.

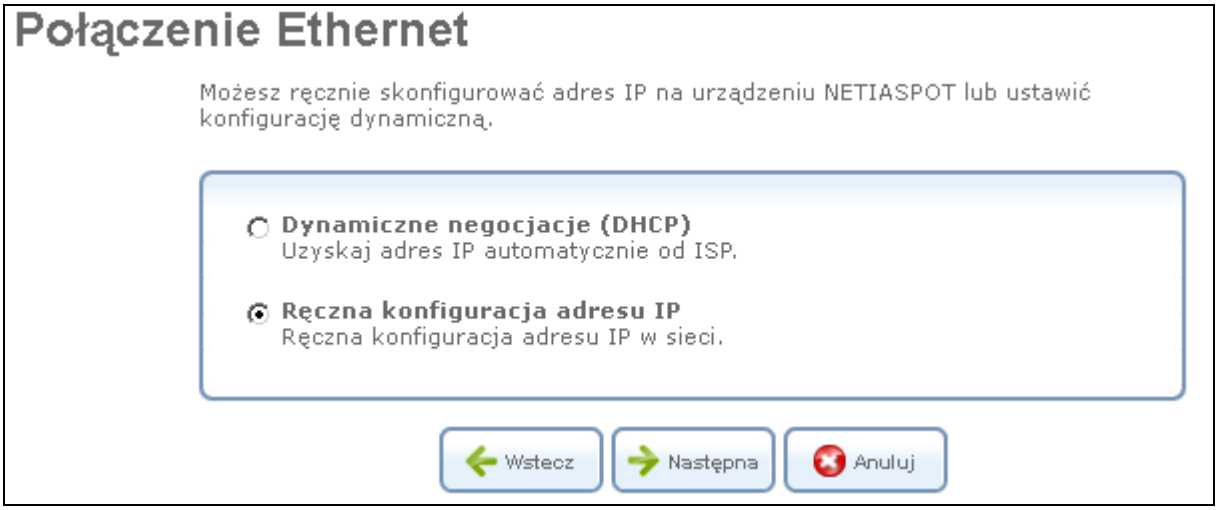
Połączenie Ethernet WAN zostanie odpowiednio skonfigurowane. Patrz sekcja 6.4.6.4, aby dowiedz się, jak przeglądać i edytować ustawienia połączenia.

6.4.6.3. Korzystanie ze statycznego adresu IP w kreatorze konfiguracji

Statyczna konfiguracja adresu IP kreatorem konfiguracji służy do konfiguracji statycznych parametrów sieci WAN.

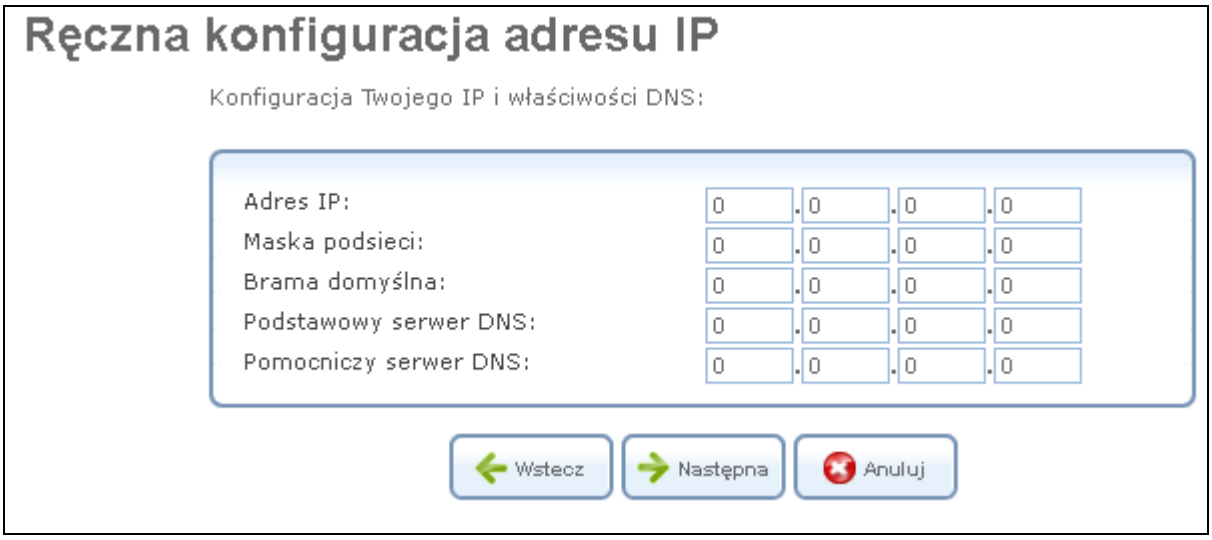
Aby statycznie skonfigurować adres IP, wykonaj następujące czynności:

1. Kliknij przycisk „Nowe połączenie" link w „Połączenia sieciowe" (patrz Rysunek 6.10). Wyświetlony zostanie „Kreator połączeń" (patrz rysunek 6.18).
2. Wybierz opcję „Połączenie z Internetem DSL", a następnie przycisk „Dalej". Wyświetlony zostanie ekran „Połączenie z Internetem DSL" (patrz rysunek 6.19).
3. Wybierz „Połączenie Ethernet", a następnie przycisk „Dalej".



Rysunek 6.96 Statyczna konfiguracja połączenia Ethernet

4. Wybierz przycisk „Ręczna konfiguracja adresu IP", a następnie przycisk „Dalej". Wyświetlony pozostanie ekran konfiguracji.



Rysunek 6.97 Statyczna konfiguracja parametrów interfejsu

5. Wpisz adres IP, maskę podsieci, bramę domyślną i adresy serwerów DNS w poszczególnych dziedzinach. Wartości te powinny być dostarczone przez Twojego ISP lub skonfigurowane przez administratora systemu.

6. Kliknij przycisk „Dalej". Wyświetlony zostanie ekran „Podsumowanie połączenia".

Rysunek 6.98 Podsumowanie połączenia

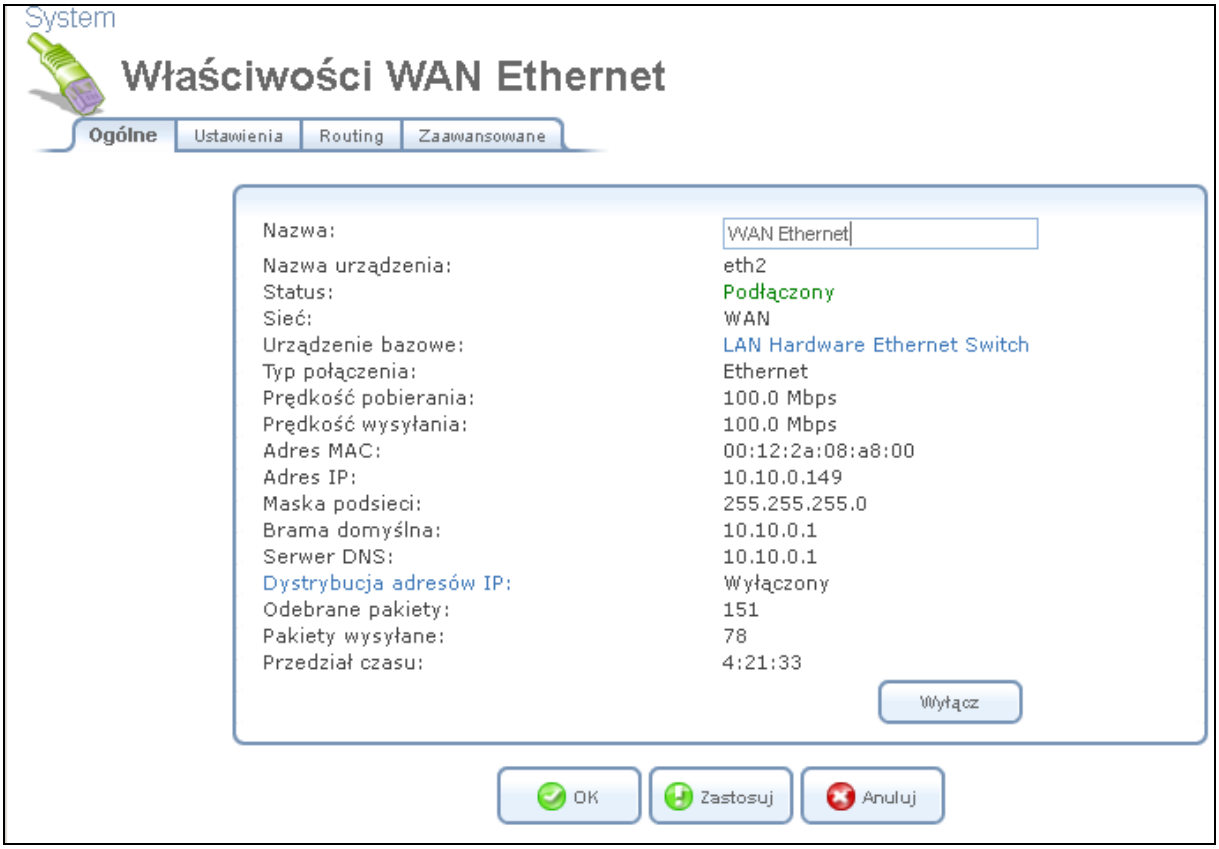
7. Wybierz pole wyboru „Edytuj nowo utworzone połączenie", a jeśli chcesz zostać skierowany na nowy ekran konfiguracji połączenia kliknij na przycisk „Koniec". Ekran ten jest opisany w dalszej części w tym rozdziale.

8. Kliknij przycisk „Koniec", aby zapisać ustawienia.

Połączenie WAN Ethernet zostanie skonfigurowane z nowymi ustawieniami. Zapoznaj się z sekcją 6.4.6.4, aby dowiedzieć się, jak przeglądać i edytować ustawienia połączenia.

6.4.6.4 Przeglądanie i edytowanie ustawień połączenia

Aby wyświetlić i zmienić ustawienia połączenia WAN Ethernet, kliknij link „WAN Ethernet w sekcji „Połączenia sieciowe". Wyświetlony zostanie ekran „Właściwości Ethernet WAN".



Rysunek 6.99 Właściwości WAN Ethernet

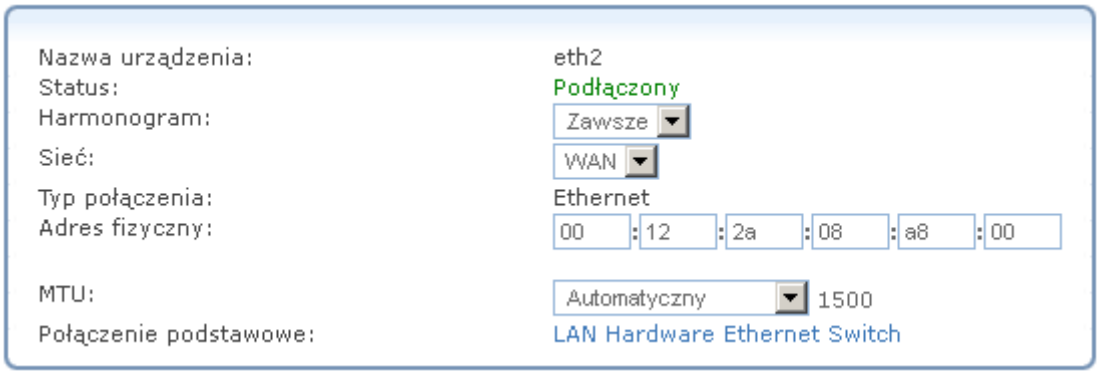
6.4.6.4.1 Ogólne

W karcie „Ogólne" możemy wyświetlić ustawienia WAN Ethernet (zob. rys. 6.99). Ustawienia te można edytować w pozostałych częściach sekcji interfejsu.

6.4.6.4.2 Ustawienia

W sekcji „Ustawienia" można skonfigurować następujące ustawienia WAN Ethernet:

Ogólne zaleca się, aby nie zmieniać wartości domyślnych, chyba że znamy zagadnienia sieciowe, które są reprezentowane w opisywanym interfejsie. Ponieważ brama jest skonfigurowana do pracy z domyślnymi wartościami, nie jest zalecana ich modyfikacja, jeśli nie jest to konieczne.



Rysunek 6.100 Ustawienia ogólne

Harmonogram - domyślnie połączenie jest zawsze aktywne. Jednakże, można skonfigurować zasady harmonogramu w celu określenia segmentów czasu, w którym połączenie może być aktywne. Po wybraniu zdefiniowanej reguły, z rozwijanego menu pozwala na wybór pomiędzy dostępnymi regułami. Aby dowiedzieć się, jak skonfigurować reguły harmonogramu, możemy odnieść się do „Definiowania reguł harmonogramu" w części administracyjnej instrukcji OpenRG.

Sieć - wybierz, czy parametry konfigurowane odnoszą się do połączenia WAN, LAN lub DMZ wybierając typ połączenia z rozwijanego menu. Aby uzyskać więcej informacji, odnoszących się do powyższej funkcji, możemy ich znaleźć w sekcji „Typy sieci" administracyjnej instrukcji OpenRG. Należy pamiętać, że przy definiowaniu połączenia sieci jako DMZ, należy także:

• Odłączyć połączenie z mostu, jeśli takie istnieje.
• Zmiana trybu połączenia trasy do „Router", w „Routingu".
• Dodaj reguły routingu na zewnątrz bramy (które mogą być dostarczane przez ISP), informuj sieć DMZ za OpenRG.

Adres fizyczny - adres fizyczny interfejsu sieciowego w sieci. Niektóre interfejsy pozwalają na zmianę tego parametru.

Klonowanie adresu MAC - naciśnij ten przycisk, aby skopiować z komputera jego aktualny adres MAC do tablicy OpenRG.

MTU - MTU jest to maksymalna jednostka transmisji. Określa ona największy rozmiar pakietu, jakim możemy przekazywać dane do Internetu. W ustawieniach domyślnych, automatycznie brama wybiera najlepsze MTU dla połączenia internetowego. Wybierz opcję „Automatycznie przez serwer DHCP", wtedy DHCP określenia wielkość MTU. W przypadku wybrania opcji „Ręcznie" zaleca się wpisać wartość od 1200 do 1500.

Protokół internetowy - wybierz jedną z następujących opcji protokołu internetowego z rozwijanego menu:

• Brak adresu IP
• Uzyskaj adres IP automatycznie
• Użyj następującego adresu IP

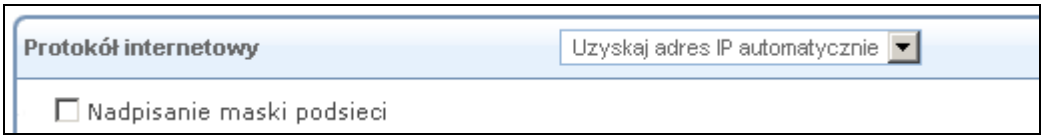
Należy pamiętać, że ekran zostanie odświeżony, aby wyświetlić odpowiednie ustawienia w zależności od wyboru.

Brak adresu IP - wybierz „Brak adresu IP", jeśli wymaga się, żeby brama nie posiadała adresu IP. Opcja ta może być użyteczna, jeśli pracujesz w środowisku, w które nie jest podłączone do innych sieci, takich jak Internet.

Rysunek 6.101 Protokół internetowy - Brak adresu IP

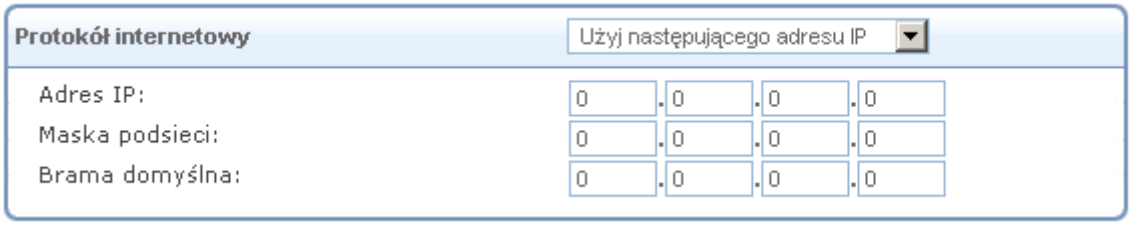
Uzyskaj adres IP automatycznie - połączenie jest domyślnie skonfigurowane do pracy jako klient DHCP. Należy zachować tą konfigurację w przypadku, gdy usługodawca obsługuje DHCP lub jeśli łączysz się za pomocą dynamicznego adresu IP. Serwer operatora, przypisuje parametry bramy adresem IP i wyznacza maskę podsieci. Możesz zmienić dynamiczną maskę podsieci przypisaną przez DHCP, wybierając opcję „Zastąp maskę podsieci" i określ własną maskę zamiast przypisanej. Można kliknąć przycisk „Zwolnij", aby

zwolnić bieżącą dzierżawę adresu IP. Po kliknięciu „Zwolnij" adres został zwolniony, należy kliknąć „Odnów". Użyj przycisku „Odnów" odnowienia dzierżawę adresu IP.



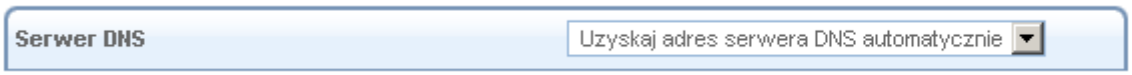
Rysunek 6.102 Automatyczne uzyskiwanie parametrów interfejsu

Użyj następującego adresu IP - połączenie można skonfigurować za pomocą stałego (statycznego) adresu IP. Usługodawca powinien zapewnić wtedy taki adresu IP i maskę podsieci.



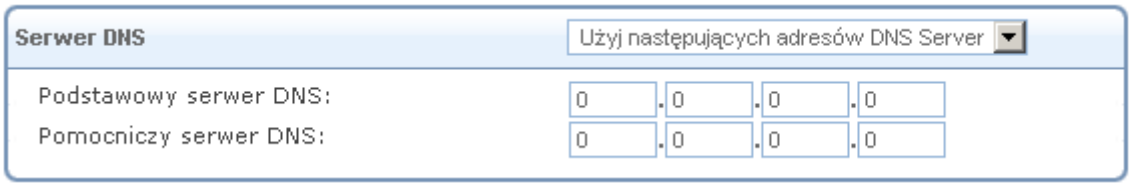
Rysunek 6.103 Protokół internetowy – Statyczne IP

Serwer DNS - Domain Name System (DNS) jest metodą, w której nazwy domeny witryny sieci www, są tłumaczone na adresy IP. Możesz skonfigurować połączenie do automatycznego uzyskania adresów serwera DNS, albo określić takiego adresy ręcznie, zgodnie z informacjami dostarczanymi przez ISP. Aby skonfigurować połączenie do automatycznego uzyskania serwera DNS, wybierz opcję „Uzyskaj adres serwera DNS automatycznie" z rozwijanego menu „Serwer DNS".



Rysunek 6.104 Serwer DNS – Automatyczne uzyskiwanie parametrów

Aby ręcznie skonfigurować adresy serwerów DNS, wybierz opcję „Użyj następujących serwerów DNS" z rozwijanego menu (patrz rysunek „Serwer DNS - Statyczne IP"). Określ do dwóch różnych adresów serwera DNS, pierwotny i zapasowy.



Rysunek 6.105 Serwer DNS - Statyczne IP

Dystrybucja adresów IP - sekcja „Dystrybucja adresów IP" pozwala skonfigurować serwer „Dynamic Host Configuration Protocol" (DHCP). Serwer DHCP automatycznie przypisuje adresy IP do komputerów w sieci. Po włączeniu tej funkcji, upewnij się, że także komputery są skonfigurowane jako klienci DHCP. Obszerny opis tej funkcji, patrz punkt 5.6. Wybierz jedną z następujących opcji z rozwijanego menu „Dystrybucja adresów IP":

Serwer DHCP

W przypadku wybranego serwera DHCP, należy wpisać następujące pola:

Początkowy adres IP - pierwszy adres IP, który może być przydzielony do komputera LAN. Domyślny adres interfejsu LAN to 192.168.1.254, zaleca się, żeby pierwszy adres IP przypisany do hosta sieci LAN to 192.168.1.2 lub wyżej.

Końcowy adres IP - końcowy adres IP z zakresu, który może być używany do automatycznego przypisywania adresów IP do komputerów z sieci lokalnej.

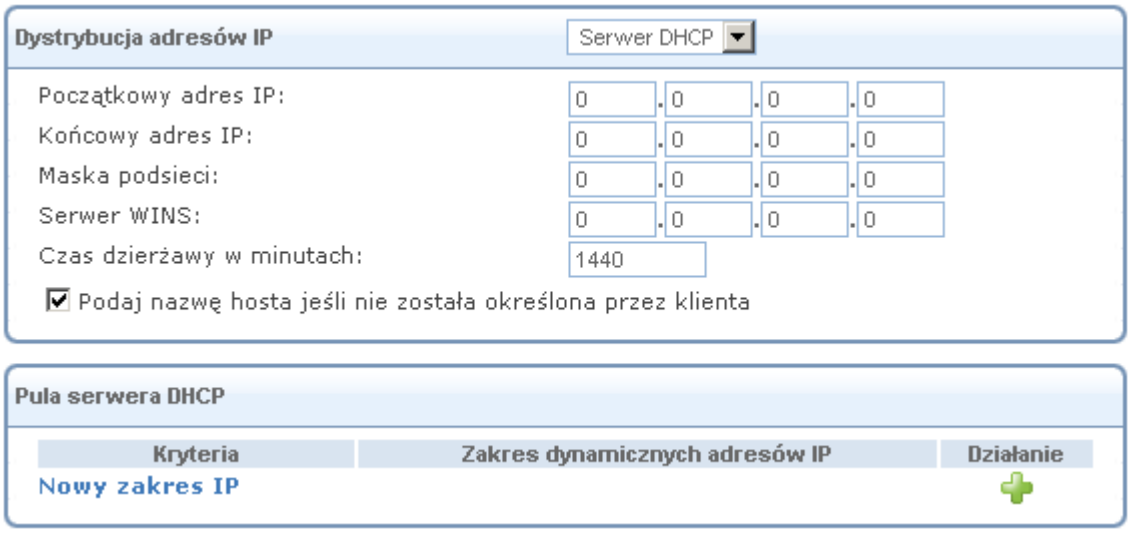
Maska podsieci -maska służy do określenia, do jakiej podsieci należy adres IP. Przykładowa domyślna wartość maski podsieci to 255.255.255.0.

Serwer WINS - jeśli chcesz korzystać z zewnętrznego serwera WINS, należy wpisać jego adres IP i kliknąć „OK".

Czas dzierżawy w minutach - każdemu urządzeniu będzie przypisany adres IP przez serwer DHCP na określony czas, gdy łączy się z siecią. Po wygaśnięciu dzierżawy serwer będzie ustalał, czy komputer jest odłączony od sieci. Jeśli tak, serwer może przypisać adres

IP do komputera nowo podłączonego. Funkcja ta zapewnia, że adresy IP, które nie są w użyciu będą dostępne dla innych komputerów w sieci.

Podaj nazwę hosta jeśli nie zostanie podana przez klienta - jeśli klient DHCP nie ma nazwy hosta, brama będzie automatycznie przypisać taką nazwę dla niego.



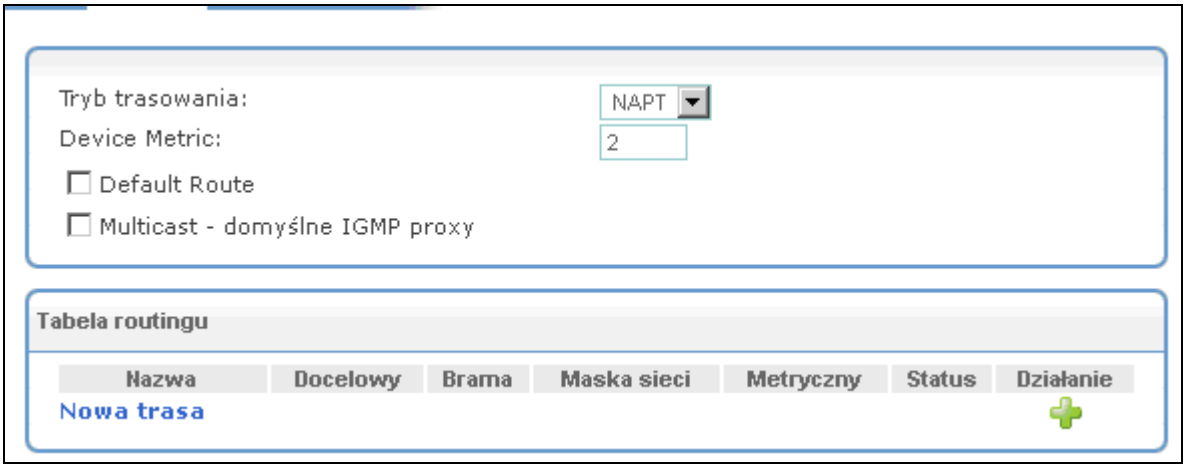
Rysunek 6.106 Dystrybucja adresów IP – Serwer DHCP

Wyłączony - wybierz opcję „Wyłączony" z rozwijanego menu, jeśli chcieliby Państwo statycznie przypisać adresy IP do komputerów w sieci.

Rysunek 6.107 Dystrybucja adresów IP – Wyłączone DHCP

6.4.6.4.3 Trasowanie

Ta zakładka umożliwia skonfigurowanie ustawień trasowania połączenia. Można wybrać i skonfigurować bramę do statycznego lub dynamicznego routingu. Routing dynamiczny automatycznie dostosowuje tablice trasowania do ruchu pakietów w sieci. Routing statyczny określa stałą ścieżkę do innych podsieci.



Rysunek 6.108 Zaawansowane właściwości trasowania

Możesz skonfigurować następujące ustawienia:

Tryb trasowania - wybierz jeden z następujących trybów trasy:

Trasa - użyj tej funkcji, jeśli chcesz , aby brama działania jako router między dwoma sieciami.

NAPT - Network Address Port Translation (NAPT) odnosi się do procesu translacji adresów z udziałem mapowania numerów portów, dzięki czemu wiele maszyn przy posiadaniu jednego publicznego adresu IP. Użyj NAPT, jeśli LAN obejmuje wiele urządzeń, topologii, które wymagają tłumaczenia port oprócz translacji adresów.

Device metric (metryka urządzenia)- jest wartością używaną przez bramę w celu określenia, czy jedna trasa jest lepsza od innej, biorąc pod uwagę takie parametry jak przepustowość, opóźnienie i wiele innych.

Trasa domyślna - zaznacz to pole wyboru w celu określenia tego urządzenia jako domyślnej trasy.

Multicast - domyślne proxy IGMP - OpenRG służy jako serwer proxy IGMP, wydawanie przyjmowanych komunikatów IGMP w imieniu podłączonych komputerów z sieci lokalnej.

To pole wyboru jest aktywne domyślnie w sieci LAN, co oznacza, że jeśli serwer multicast jest dostępny w LAN, inne komputery z sieci LAN wyślą prośbę, aby dołączyć do grup multicast (wyślą żądanie IGMP). Jednak to pole wyboru jest wyłączone domyślnie dla połączenia WAN, co oznacza, że komputery z sieci lokalnej nie będą w stanie dołączyć do grupy multicast WAN serwerów multicast. Podczas tworzenia mostu sieciowego WAN-LAN, to pole wyboru musi być odznaczone.

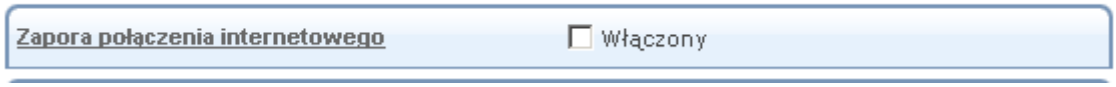
Wersja IGMP Query - OpenRG obsługuje wszystkie trzy wersje IGMP. Wybierz wersję, której chcesz użyć. Pamiętaj, że menu rozwijane pojawia się tylko podczas połączenia LAN.

Tabela routingu - umożliwia dodanie lub zmianę trasy, gdy urządzenie jest aktywne. Użyj przycisku „Nowa trasa", aby dodać trasy lub edytować istniejące trasy.

6.4.6.4.4 Zaawansowane

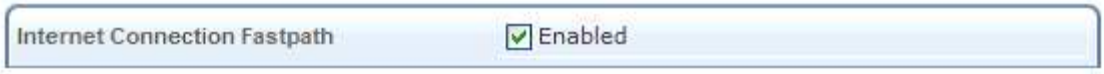
Ta sekcja pozwala skonfigurować ustawienia zaawansowane interfejsu WAN Ethernet.

• **Zapora połączenia internetowego** - Twoja zapora sieciowa urządzenia pomaga chronić komputer poprzez zapobieganie nieautoryzowanym uzyskaniem dostępu przez użytkowników za pośrednictwem sieci, takiej jak Internet. Zapora sieciowa może być aktywowana na danym połączeniu sieciowym. Aby włączyć zapory dla połączenia sieciowego, zaznacz pole wyboru „Włączony". Aby dowiedzieć się jak najwięcej na temat zabezpieczeń bramy, patrz punkt 5.2.



Rysunek 6.109 Zapora połączenia internetowego

Internetowe połączenie FastPath - zaznaczenie tego pola wyboru pozwala wykorzystać algorytm FastPath dla zwiększenia przepływu pakietów, co skutkuje szybszą komunikacją pomiędzy siecią LAN i WAN. Domyślnie ta funkcja jest włączona.



Rysunek 6.110 Internetowe połączenie FastPath

• **Dodatkowe adresy IP** - można dodać aliasy (dodatkowe adresy IP) bramy, klikając na link „Nowy adres IP". Pozwala to dostępu do bramy za pomocą aliasów oprócz domyślnego 192.168.1.254 i http://netiaspot.home.

Rysunek 6.111 Dodatkowe adresy IP

6.4.7. Konfiguracja ustawień sieci WAN DSL

Opcja WAN DSL umożliwia nawiązanie fizycznego połączenia między bramą a siecią operatora za pomocą kabla telefonicznego podłączonego do portu bramy DSL i gniazdka telefonicznego. Aby przeglądać i edytować ustawienia bramy WAN DSL, kliknij link „WAN DSL" w „Połączenia sieciowe" (patrz rysunek 6.10). Wyświetlony zostanie ekran „Właściwości WAN DSL".

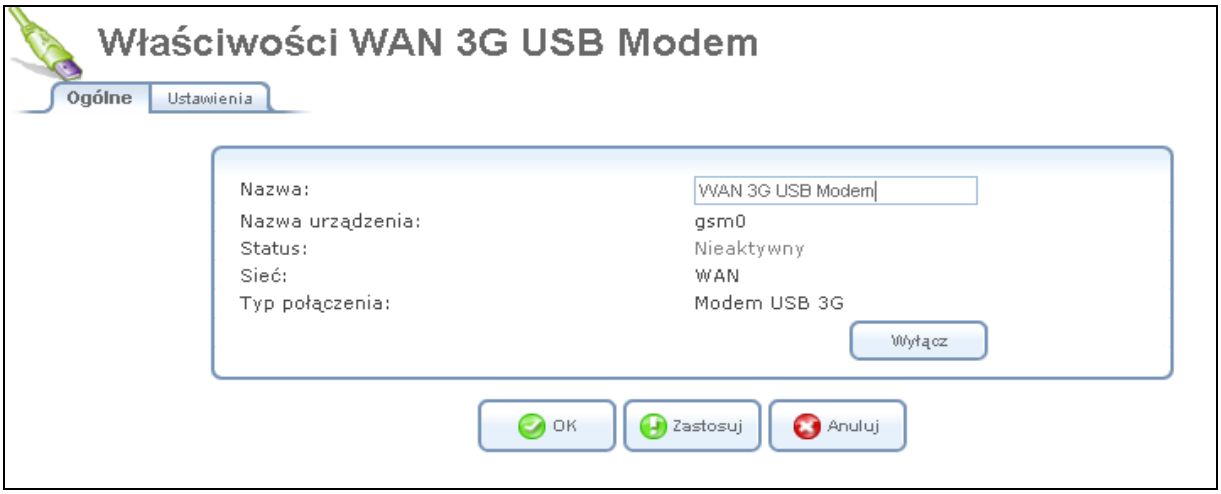
Rysunek 6.112 Właściwości połączenia WAN DSL

Ten ekran umożliwia wyświetlanie parametrów WAN DSL i status interfejsu DSL, pozwala także zmienić nazwę i wyłączyć interfejs WAN DSL.

6.4.8. WAN 3G

Połączenie WAN 3G za pomocą urządzenia modemu USB, który pozwala na utworzenie fizycznego połączenia między bramą a siecią operatora za pomocą urządzenia/modemu sieci komórkowej 3G, który możemy podłączyć do portu USB OpenRG.

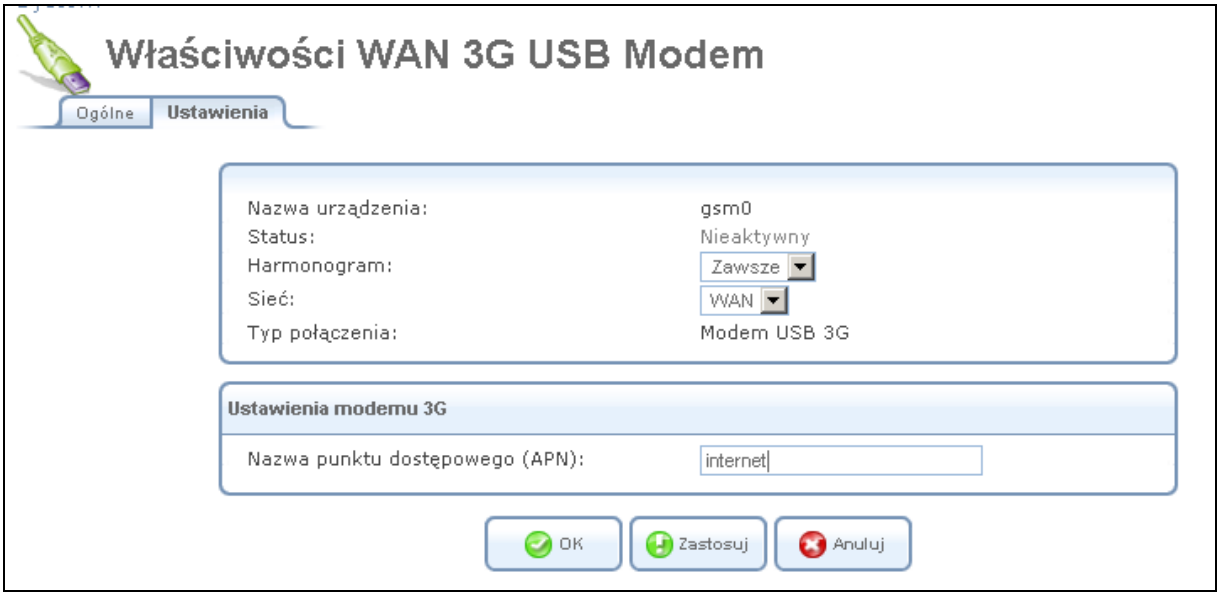
Aby przeglądać i edytować ustawienia WAN 3G, należy kliknąć na link „Właściwości serial PPP" w sekcji „Połączenia sieciowe".



Rysunek 6.113 Właściwości połączenia 3G

Ogólne – sekcja „Ogólne" umożliwia wyświetlanie parametrów połączenia „WAN 3G" i jego status, a także pozwala zmienić nazwę i wyłączyć interfejs 3G WAN.

Ustawienia - sekcja „Ustawienia" umożliwia zmianę nazwy punktu dostępu 3G (APN)



Rysunek 6.114 Ustawienia - Właściwości WAN 3G

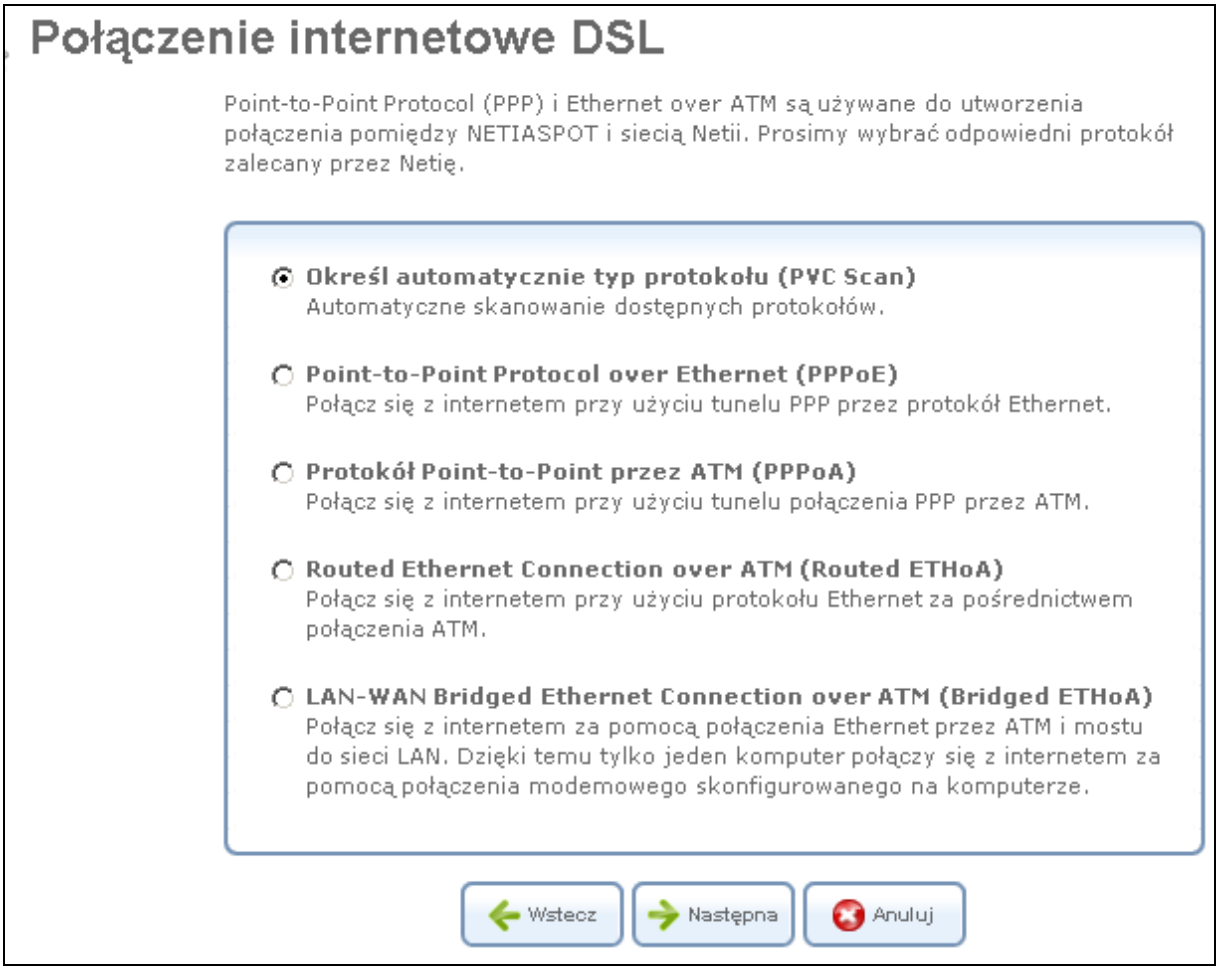
Zaleca się nie zmieniać wartości domyślnych, jeśli tematyka opisywanej sekcji nie jest nam znana. Ponieważ brama jest skonfigurowana do pracy z wartościami domyślnymi, zmiana parametrów nie jest konieczna do poprawnej pracy urządzenia.

6.4.9. Ustalenie parametrów VPI/VCI połączenia DSL

Narzędzie kreatora dostępnego połączenia określi typ protokółu automatycznie (PVC Scan), pozwala na automatyczne skanowanie pary VCI/VPI, są to niezbędne parametry przy połączeniu z DSL. W przypadku takich par, gdzie nie zostaną znalezione, usługodawca powinien dostarczyć odpowiednie dane.

Aby automatycznie wyszukać pary VPI/VCI, wykonaj następujące czynności:

1. Kliknij przycisk „Nowe połączenie" link w ekranie „Połączenia sieciowe". Wyświetlony zostanie ekran kreatora połączenia (patrz rysunek 6.18).
2. Wybierz „Połączenie z internetem DSL", a następnie przycisk „Dalej" (patrz rysunek 6.19).

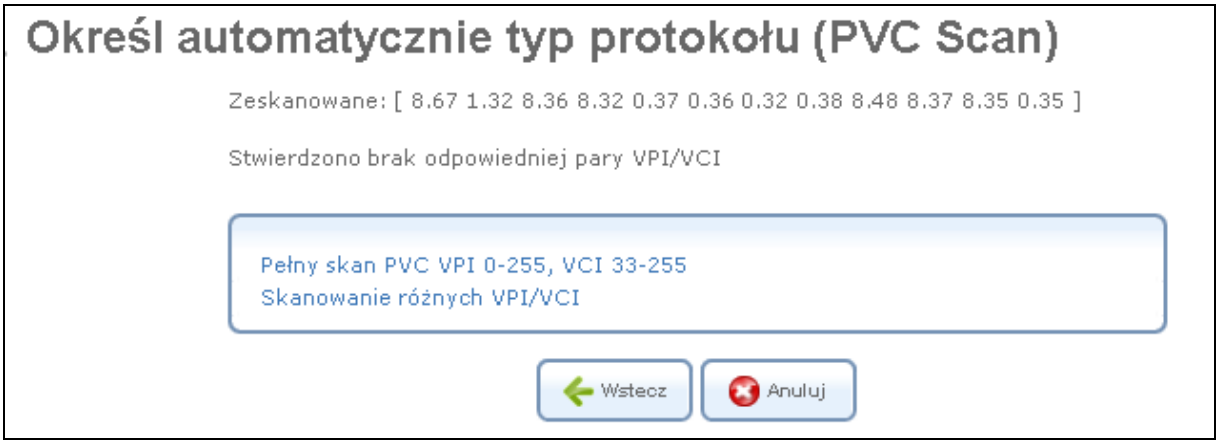


3. Wybierz „Określ automatycznie typ protokołu (PVC Scan)", a następnie kliknij na przycisk „Dalej". Skanowanie rozpocznie się odświeżania ekranu co kilka sekund, aby wyświetlić postęp.

Rysunek 6.115 Określenie automatycznego typu protokołu

Po zakończeniu skanowania, wyświetlony zostanie komunikat informujący o sukcesie lub niepowodzeniu skanowania.

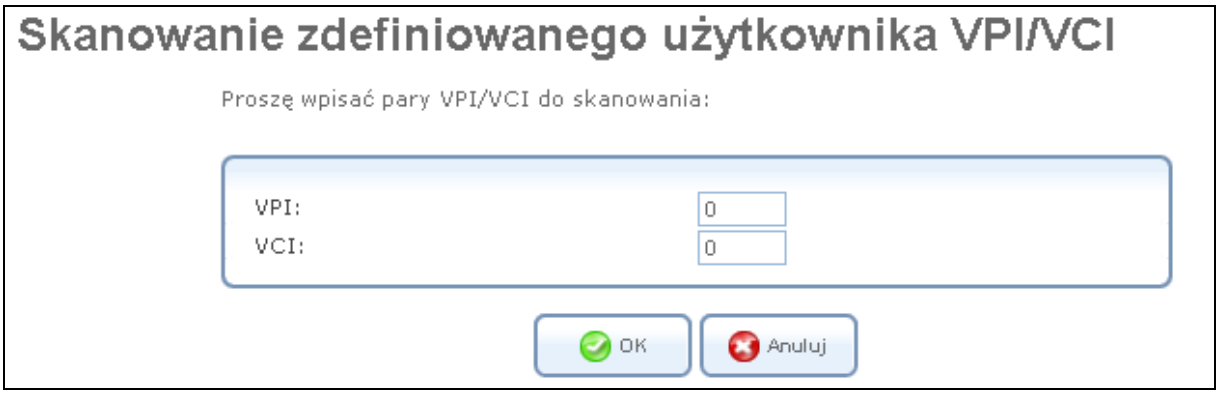
4. Jeśli skanowanie się nie udało, na ekranie przedstawione zostaną następujące opcje:



Rysunek 6.116 Skanowanie PVC – przedstawia ekran niepowodzenia skanowania

• Pełne skanowanie PVC 0-255 VPI, VCI 33-255 – kliknij na ten link, aby rozpocząć dłuższe, bardziej dokładne skanowanie, między VPI i VCI 33-255 0-255.

• Różne skanowanie VPI/VCI - kliknij na ten link do skanowania w poszukiwaniu konkretnej pary VPI/VCI. Ekran „Skanuj zdefiniowane przez użytkownika VPI/VCI" (patrz rys. 6.117). Wpisz pary VPI/VCI, które chcesz przeskanować i kliknij „OK".



Rysunek 6.117 Zdefiniowane skanowanie VPI/VCI

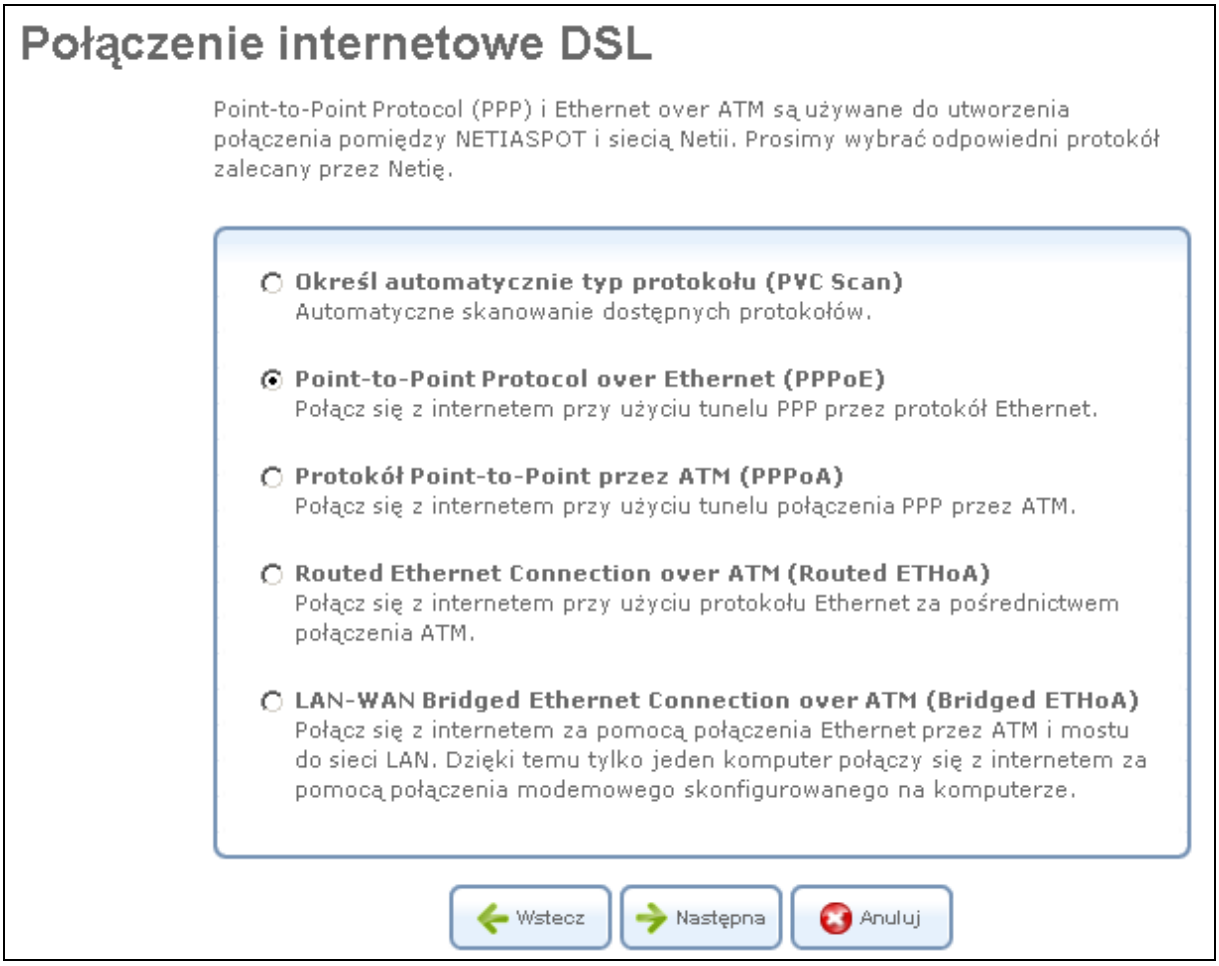
6.4.10 Konfiguracja połączenia PPPoE

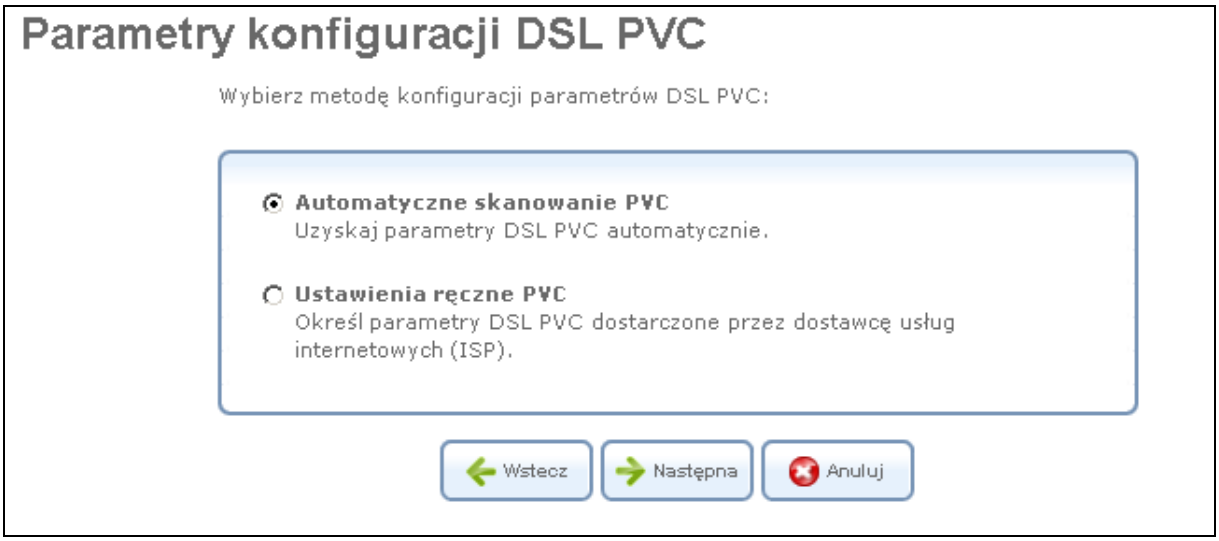
Połączenie Point-to-Point Protocol przez Ethernet (PPPoE) opiera się na dwóch szeroko akceptowanych standardach, PPP i Ethernet. PPPoE umożliwia komputerom sieci domowej, które komunikują się w sieci Ethernet wymianę informacji z komputerami w Internecie. Protokół PPPoE wspiera warstwy i uwierzytelnianie szeroko stosowane w PPP, umożliwia pracę połączeń punkt-punkt, umożliwia pracę w wielopunktowej architekturze Ethernet. PPPoE określa adres MAC Ethernet zdalnego urządzenia, w celu ustanowienia sesji.

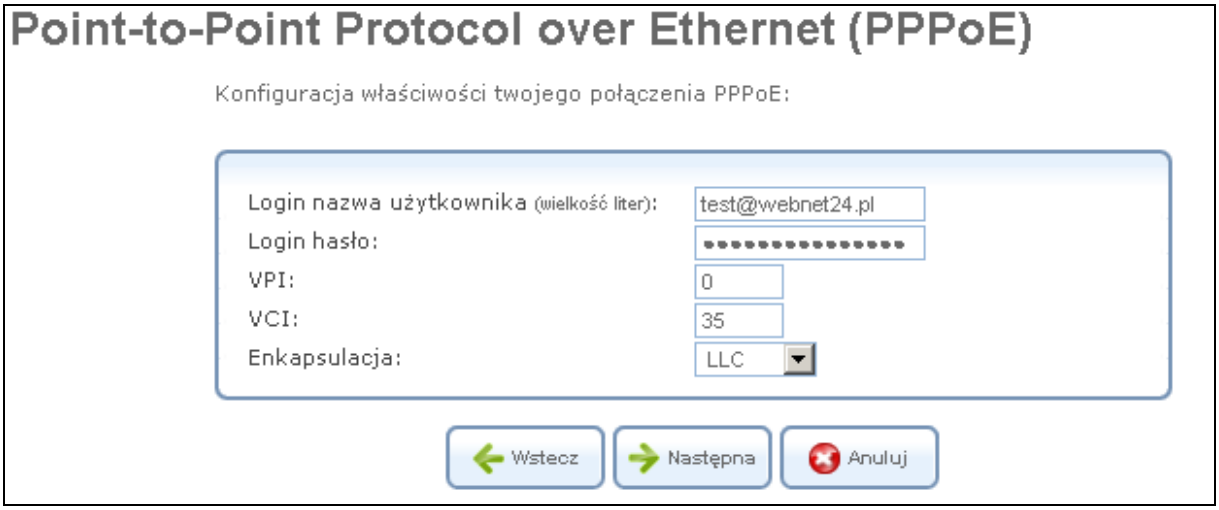
6.4.10.1 Tworzenie połączenia PPPoE

Aby utworzyć połączenie PPPoE, wykonaj następujące czynności:

1. Kliknij na przycisk „Nowe połączenie" link w sekcji „Połączenia sieciowe" (patrz rysunek 6.10). Wyświetlony zostanie ekran kreatora połączeń (patrz rysunek 6.18).
2. Wybierz „Połączenie z Internetem DSL", a następnie przycisk „Dalej" (patrz rysunek 6.19).
3. Wybierz „Point-to-Point Protocol over Ethernet", a następnie kliknij przycisk „Dalej".

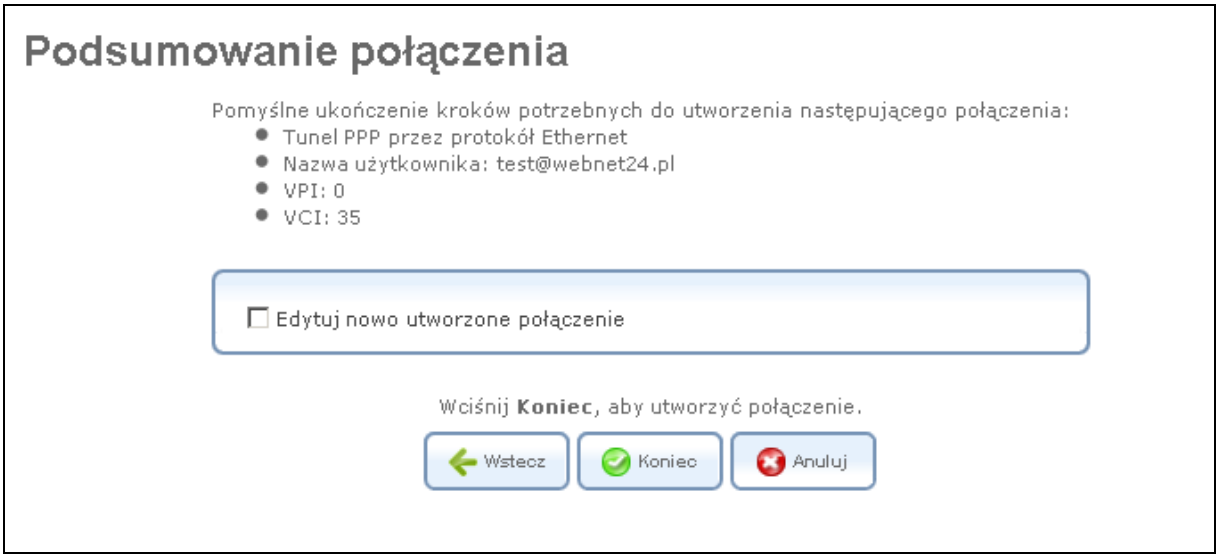

Połączenie internetowe DSL
Point-to-Point Protocol (PPP) i Ethernet over ATM są używane do utworzenia połączenia pomiędzy NETIASPOT i siecią Netii. Prosimy wybrać odpowiedni protokół zalecany przez Netię.
Określ automatycznie typ protokołu (PVC Scan)
Automatyczne skanowanie dostępnych protokołów.
Point-to-Point Protocol over Ethernet (PPPoE)
Połącz się z internetem przy użyciu tunelu PPP przez protokół Ethernet.
Protokół Point-to-Point przez ATM (PPPoA)
Połącz się z internetem przy użyciu tunelu połączenia PPP przez ATM.
Routed Ethernet Connection over ATM (Routed ETHoA)
Połącz się z internetem przy użyciu protokołu Ethernet za pośrednictwem połączenia ATM.
LAN-WAN Bridged Ethernet Connection over ATM (Bridged ETHoA)
Połącz się z internetem za pomocą połączenia Ethernet przez ATM i mostu do sieci LAN. Dzięki temu tylko jeden komputer połączy się z internetem za pomocą połączenia modemowego skonfigurowanego na komputerze.
Wstecz
Następna
Anuluj


Parametry konfiguracji DSL PVC
Wybierz metodę konfiguracji parametrów DSL PVC:
Automatyczne skanowanie PVC
Uzyskaj parametry DSL PVC automatycznie.
Ustawienia ręczne PVC
Określ parametry DSL PVC dostarczone przez dostawcę usług internetowych (ISP).
Wstecz
Następna
Anuluj



Rysunek 6.118 Point-to-Point Protocol przez Ethernet (PPPoE)

4. Wprowadź nazwę użytkownika i hasło dostarczone przez dostawcę usług internetowych (ISP), a następnie kliknij „Dalej". Wyświetlony zostanie ekran „Podsumowanie połączenia".



Rysunek 6.119 Podsumowanie połączenia

5. Wybierz pole wyboru „Edytuj nowo utworzonego połączenie", jeśli nie chcesz być skierowany do nowego ekranu konfiguracji połączenia kliknij „Koniec". Sekcja została opisana w dalszej części tego rozdziału.

6. Kliknij przycisk „Zakończ", aby zapisać ustawienia.

Nowe połączenie PPPoE zostanie dodane do listy połączeń sieciowych i będzie konfigurowalne jak każde inne połączenie.

Uwaga: Jeśli połączenie WAN jest ustawione jako PPPoE, gdy nie ma aktywnego serwera PPPoE, a serwer DHCP jest dostępny, urządzenia wyświetli status „W trakcie - znaleziono serwer DHCP, rozważ konfigurację połączenia WAN w trybie automatycznym".

6.4.10.2 Przeglądanie i edytowania ustawień połączeń

Aby wyświetlić i zmienić ustawienia połączenia PPPoE, należy kliknąć na link „WAN PPPoE" w sekcji „Połączenia sieciowe" (patrz Rysunek 6.10). Wyświetlony zostanie ekran „Właściwości WAN PPPoE".

Rysunek 6.120 Właściwości połączenia PPPoE

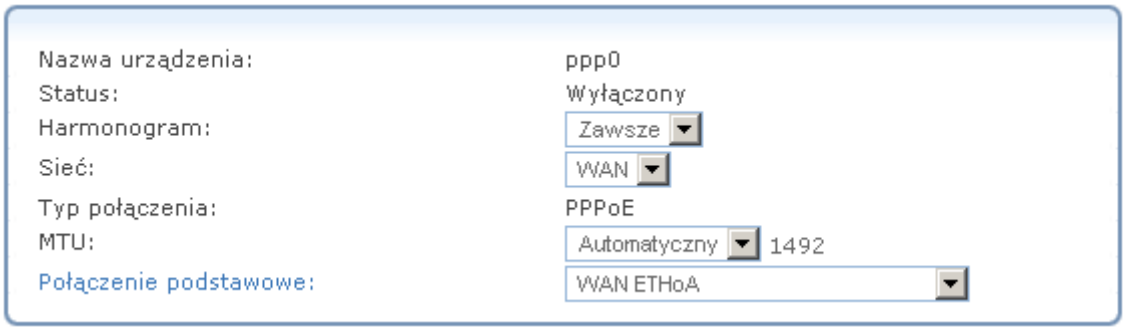
6.4.10.2.1 Ogólne

Ta sekcja umożliwia wyświetlanie ustawień połączenia PPPoE (patrz rys. 6.120). Wprowadzone ustawienia mogą być edytowane w pozostałej sekcji interfejsu, jak opisano w następujących sekcjach.

6.4.10.2.2 Ustawienia

Sekcja „Ustawienia" pozwala modyfikować następujące ustawienia PPPoE:

Ogólne - ta sekcja wyświetla ogólne parametry połączenia.



Rysunek 6.121 Ogólne ustawienia PPPoE

Harmonogram - domyślnie połączenie jest zawsze aktywne. Jednakże, można skonfigurować zasady harmonogramu w celu określenia segmentów czasu, w którym połączenie może być aktywne. Po wybraniu zdefiniowanej reguły, z rozwijanego menu pozwala na wybór pomiędzy dostępnymi regułami. Aby dowiedzieć się jak skonfigurować reguły harmonogramu, możemy odnieść się do „Definiowania reguł harmonogramu" w części administracyjnej instrukcji OpenRG.

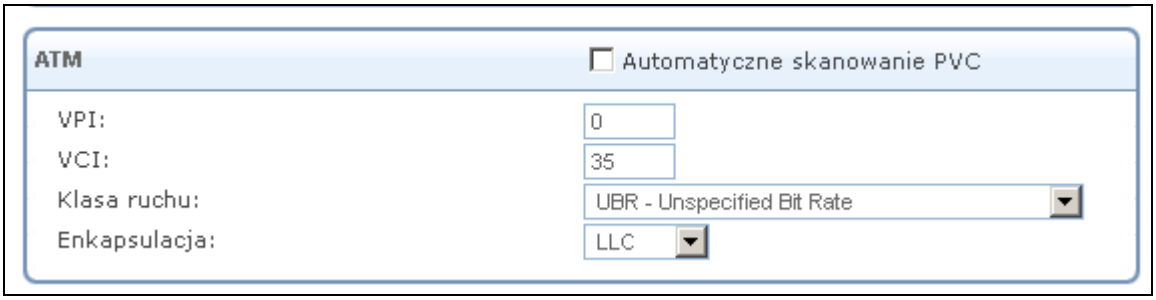
Sieć - wybierz, czy parametry konfigurowane odnoszą się do połączenia WAN, LAN lub DMZ wybierając typ połączenia z rozwijanego menu. Aby uzyskać więcej informacji, odnoszących się do powyższej funkcji, możemy ich znaleźć w sekcji „Typy sieci" administracyjnej instrukcji OpenRG. Należy pamiętać, że przy definiowaniu połączenia sieci jako DMZ, należy także:

• Odłączyć połączenie z mostu, jeśli takie istnieje.
• Zmiana trybu połączenia trasy do „Router", w „Routingu".
• Dodaj reguły routingu na zewnątrz bramy (które mogą być dostarczane przez ISP), informuj sieć DMZ za OpenRG.

MTU - MTU jest to maksymalna jednostka transmisji. Określa ona największy rozmiar pakietu, jakim możemy przekazywać dane do Internetu. W ustawieniach domyślnych, automatycznie brama wybiera najlepsze MTU dla połączenia internetowego. Wybierz opcję „Automatycznie przez serwer DHCP", wtedy DHCP określenia wielkość MTU. W przypadku wybrania opcji „Ręcznie" zaleca się wpisać wartość od 1200 do 1500.

Połączenie bazowe - określa podstawowe połączenia, powyżej którego protokół będzie zainicjowany.

ATM - Asynchronous Transfer Mode (ATM) to technologia oparta na przesyłania danych w sieciach komórkowych lub pakietów o stałej wielkości. Używane komórki ATM są stosunkowo niewielkie w porównaniu do jednostek używanych w innych technologiach. Mała, stała wielkość komórek pozwala na transmisję wideo, audio i danych komputerowych, zapewniając, że żaden pojedynczy typ danych nie zużyje połączenia. Adresowanie ATM składa się z dwóch identyfikatorów, które określają ścieżkę wirtualną (VPI) i wirtualne połączenie (VCI). Ścieżka wirtualna składa się z wielu kanałów wirtualnych do tego samego punktu końcowego. Enkapsulacja do połączenia powinna być ustawiona jako „LLC" lub „VCMux". Należy skonfigurować te parametry zgodnie z informacjami przekazanymi przez ISP.



Rysunek 6.122 Ustawienia ATM

Protokół internetowy - wybierz jedną z następujących opcji protokołu internetowego

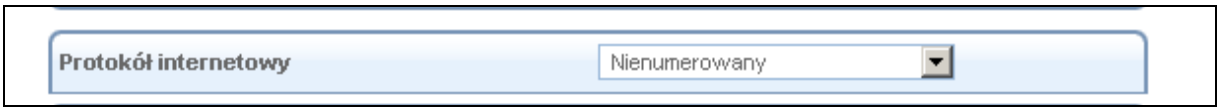
• Nienumerowany

• Uzyskaj adres IP automatycznie

• Użyj następującego adresu IP

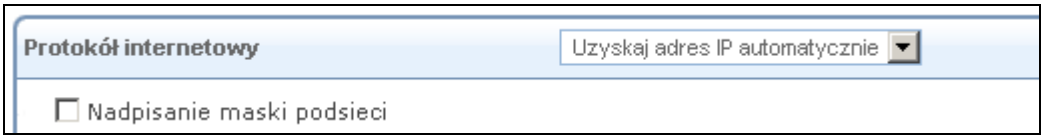
Zwróć uwagę, że ekran zostanie odświeżony, aby wyświetlić odpowiednie ustawienia zgodnie z Twoim wyborem.

Nienumerowany - wybierz tę opcję, aby przypisać wstępnie adres LAN jako adres WAN OpenRG. Jest to przydatne podczas, gdy OpenRG pracuje w trybie routingu. Przed wybraniem tej opcji należy, skonfigurować sekcję „Protokół internetowy" urządzenia sieci LAN (lub most sieciowy w przypadku, gdy urządzenie LAN jest mostem sieciowym) użyć statycznego adresu IP z zakresu adresów IP dostarczonych przez usługodawcę internetowego (zamiast 192.168.1.254).



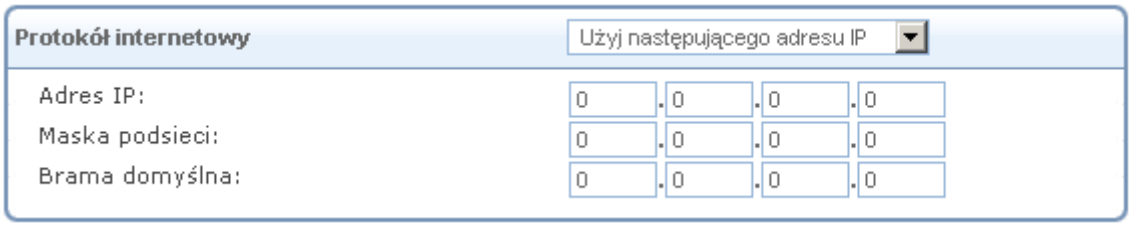
Rysunek 6.123 Protokół internetowy – nienumerowany

Uzyskaj adres IP automatycznie - połączenie jest domyślnie skonfigurowane do pracy jako klient DHCP. Należy zachować tą konfigurację w przypadku, gdy usługodawca obsługuje DHCP lub jeśli łączysz się za pomocą dynamicznego adresu IP. Serwer operatora, przypisuje parametry bramy adresem IP i wyznacza maskę podsieci. Możesz zmienić dynamiczną maskę podsieci przypisaną przez DHCP, wybierając opcję „Zastąp maskę podsieci" i określ własną maskę zamiast przypisanej. Można kliknąć przycisk „Zwolnij", aby zwolnić bieżącą dzierżawę adresu IP. Po kliknięciu „Zwolnij" adres został zwolniony, należy kliknąć „Odnów". Użyj przycisku „Odnów" odnowienia dzierżawę adresu IP.



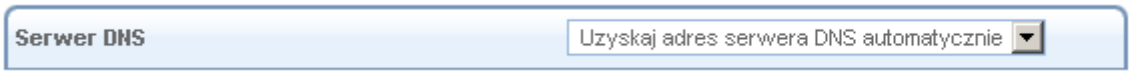
Rysunek 6.124 Automatyczne uzyskiwanie parametrów interfejsu

Użyj następującego adresu IP - połączenie można skonfigurować za pomocą stałego (statycznego) adresu IP. Usługodawca powinien zapewnić wtedy taki adresu IP i maskę podsieci.



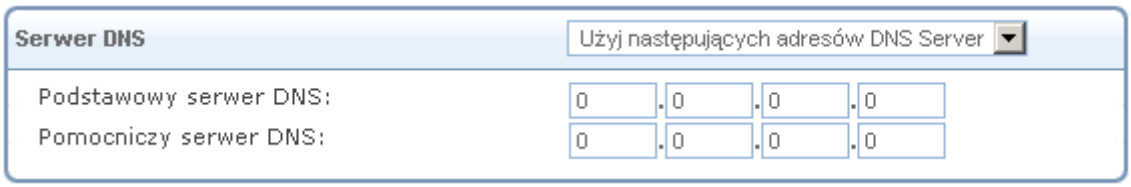
Rysunek 6.125 Protokół internetowy – Statyczne IP

Serwer DNS - Domain Name System (DNS) jest metodą, w której nazwy domeny witryny sieci www są tłumaczone na adresy IP. Możesz skonfigurować połączenie do automatycznego uzyskania adresów serwera DNS, albo określić takiego adresy ręcznie, zgodnie z informacjami dostarczanymi przez ISP. Aby skonfigurować połączenie do automatycznego uzyskania serwera DNS, wybierz opcję „Uzyskaj adres serwera DNS automatycznie" z rozwijanego menu „Serwer DNS".



Rysunek 6.126 Serwer DNS – Automatyczne uzyskiwanie parametrów

Aby ręcznie skonfigurować adresy serwerów DNS, wybierz opcję „Użyj następujących serwerów DNS" z rozwijanego menu (patrz rysunek „Serwer DNS - Statyczne IP"). Określ do dwóch różnych adresów serwera DNS, pierwotny i zapasowy.

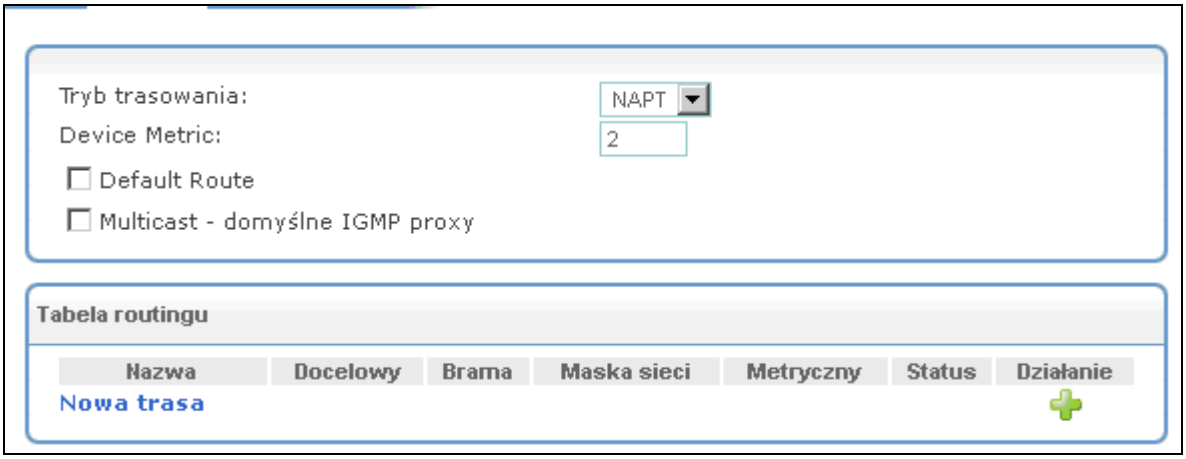


Rysunek 6.127 Serwer DNS - Statyczne IP

6.4.10.2.3 Trasowanie

Ta zakładka umożliwia skonfigurowanie ustawień trasowania połączenia. Można wybrać i skonfigurować bramę do statycznego lub dynamicznego routingu. Routing dynamiczny

automatycznie dostosowuje tablice trasowania do ruchu pakietów w sieci. Routing statyczny określa stałą ścieżkę do innych podsieci.



Rysunek 6.128 Zaawansowane właściwości trasowania

Możesz skonfigurować następujące ustawienia:

Tryb trasowania - wybierz jeden z następujących trybów trasy:

Trasa - użyj tej funkcji, jeśli chcesz , aby brama działania jako router między dwoma sieciami.

NAPT - Network Address Port Translation (NAPT) odnosi się do procesu translacji adresów z udziałem mapowania numerów portów, dzięki czemu wiele maszyn przy posiadaniu jednego publicznego adresu IP. Użyj NAPT, jeśli LAN obejmuje wiele urządzeń, topologii, które wymagają tłumaczenia port oprócz translacji adresów.

Device metric (metryka urządzenia)- jest wartością używaną przez bramę w celu określenia, czy jedna trasa jest lepsza od innej, biorąc pod uwagę takie parametry jak przepustowość, opóźnienie i wiele innych.

Trasa domyślna - zaznacz to pole wyboru w celu określenia tego urządzenia jako domyślnej trasy.

Multicast - domyślne proxy IGMP - OpenRG służy jako serwer proxy IGMP, wydawanie przyjmowanych komunikatów IGMP w imieniu podłączonych komputerów z sieci lokalnej. To pole wyboru jest aktywne domyślnie w sieci LAN, co oznacza, że jeśli serwer multicast jest dostępny w LAN, inne komputery z sieci LAN wyślą prośbę, aby dołączyć do grup multicast (wyślą żądanie IGMP). Jednak to pole wyboru jest wyłączone domyślnie dla połączenia WAN, co oznacza, że komputery z sieci lokalnej nie będą w stanie dołączyć do grupy multicast WAN serwerów multicast. Podczas tworzenia mostu sieciowego WAN-LAN, to pole wyboru musi być odznaczone.

Wersja IGMP Query - OpenRG obsługuje wszystkie trzy wersje IGMP. Wybierz wersję, której chcesz użyć. Pamiętaj, że menu rozwijane pojawia się tylko podczas połączenia LAN.

Tabela routingu - umożliwia dodanie lub zmianę trasy, gdy urządzenie jest aktywne. Użyj przycisku „Nowa trasa", aby dodać trasy lub edytować istniejące trasy.

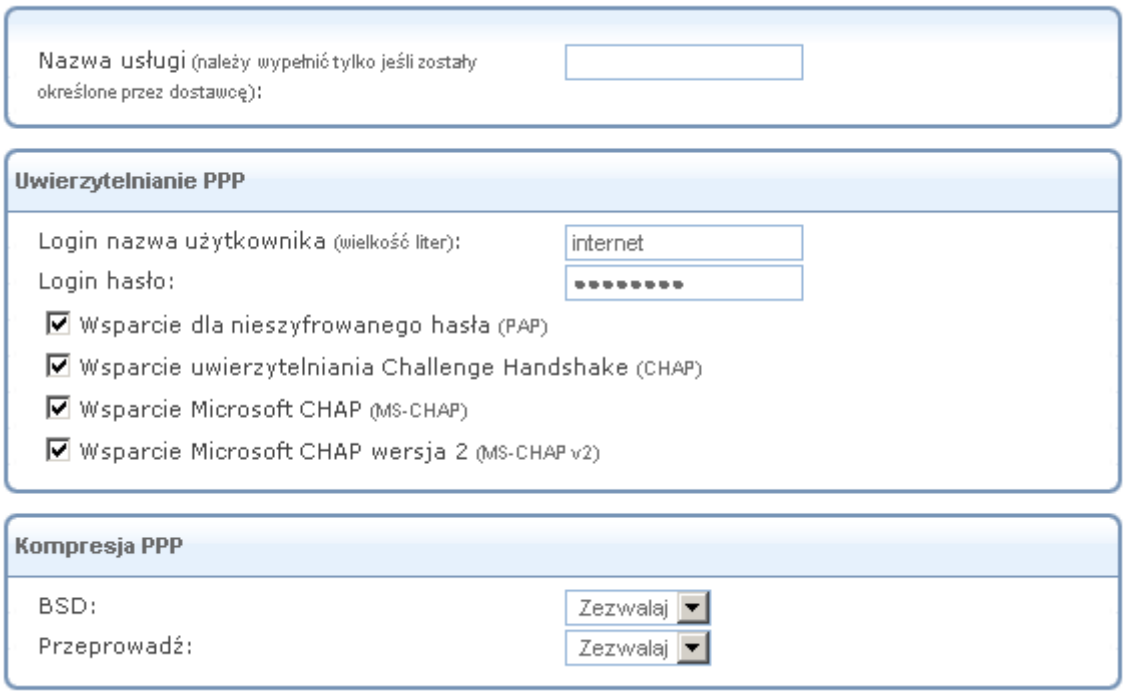
6.4.10.2.4 PPP

Point-to-Point Protocol (PPP) jest najbardziej popularną metodą transportu pakietów pomiędzy użytkownikiem a dostawcą usług internetowych. PPP obsługuje protokoły uwierzytelniania, takie jak PAP i CHAP, jak również inne takie jak kompresje i protokoły szyfrowania.

Nazwa usługi - należy podać nazwę sieci usługi, jeżeli taka nazwa została dostarczone przez ISP. Jeśli nie została podana dedykowana nazwa usługi, wtedy pozostawiamy to pole puste.

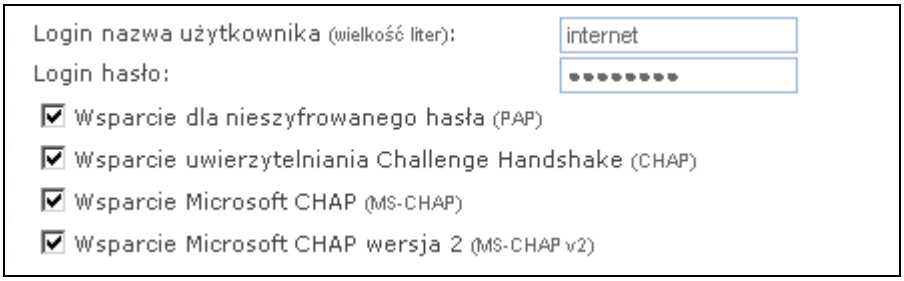
PPP na żądanie – opcja PPP na żądanie rozpoczyna sesję punkt-punkt tylko gdy pakiety są rzeczywiście wysyłane przez internet.

Czas między próbami ponownego połączenia – należy podać czas trwania między ponownym połączeniem PPP, dane jeśli będą wymagane to zostaną dostarczone przez ISP.



Rysunek 6.129 Konfiguracja PPP

Uwierzytelnianie PPP - Point-to-Point Protocol (PPP), obecnie obsługuje cztery protokoły uwierzytelniania: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) i Microsoft CHAP w wersji 1 i 2. Ta sekcja pozwala na wybranie protokołu uwierzytelniania bramy. Wybrany protokół mogą wykorzystać podczas negocjacji z serwerem PPTP. Wybierz wszystkie protokoły, jeśli nie ma dostępnych informacji na temat serwera protokołu uwierzytelniania. Uwaga - szyfrowanie odbywa się tylko wtedy, gdy wybrane są Microsoft CHAP, Microsoft CHAP wersja 2, albo zostały wybrane oba.



Rysunek 6.130 Uwierzytelnianie PPP

Login Nazwa użytkownika zgodnie z ustaleniami z ISP.

Login Hasło - zgodnie z ustaleniami z ISP.

Wsparcie niezaszyfrowanego hasła (PAP) - protokół uwierzytelniania hasła (PAP) jest prosty, schematu uwierzytelniania odbywa się zwykłym tekstem. Nazwa użytkownika i hasło są wysyłane przez sieć w postaci zwykłego tekstu. PAP nie jest bezpiecznym protokołem uwierzytelniania.

Atak „Man-in-the-middle" (człowiek pośrodku) możne określić hasło klienta dostępu zdalnego. PAP nie jest zalecany i negatywnie wpływa na nasze bezpieczeństwo.

Challenge Authentication Support Handshake (CHAP) – jest to protokół uwierzytelniania typu wyzwanie-odpowiedź, który używa hash MD5 do zabezpieczenia odpowiedzi na zapytanie. CHAP jest bezpiecznym protokołem uwierzytelniania, zapewnia ochronę przed atakami wykorzystującymi podsłuch transmisji, wykorzystuje MD5. Jest preferowany jako uwierzytelnianie w PPP.

Wsparcie Microsoft CHAP - zaznacz to pole wyboru, jeśli komunikujesz się z użytkownikami, którzy używają protokołu uwierzytelniania CHAP Microsoft.

Wsparcie Microsoft CHAP w wersji 2 - zaznacz to pole wyboru, jeśli komunikujesz się z użytkownikami, którzy używają protokołu uwierzytelniania Microsoft CHAP w wersji 2.

Kompresja PPP – „Compression Control Protocol" (CCP) jest odpowiedzialny za konfigurację, dzięki czemu umożliwiają włączenie/wyłączenie algorytmów kompresji na obu końcach połączenia punkt-punkt. Jest również używany jako mechanizm sygnalizacji awarii kompresji/dekompresji w wiarygodny sposób.

Rysunek 6.131 Kompresja PPP

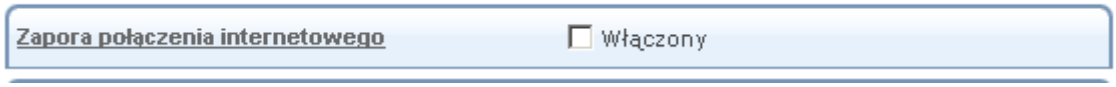
Dla każdego algorytmu kompresji, wybierz jedną z następujących opcji z menu rozwijanego:

Odrzuć - odrzucenie połączeń PPP z użytkownikami, którzy korzystają z algorytmu kompresji.
Zezwalaj - zezwalaj na połączenia PPP z użytkownikami, którzy korzystają z algorytmu kompresji.
Wymagaj - zapewniaj połączenie PPP z użytkownikami, którzy korzystają z algorytmu kompresji.

6.4.10.2.5 Zaawansowane

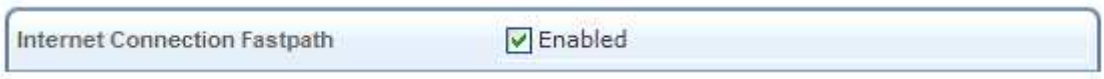
Ta sekcja pozwala skonfigurować ustawienia zaawansowane interfejsu PPPoE.

• **Zapora połączenia internetowego** - Twoja zapora sieciowa urządzenia pomaga chronić komputer poprzez zapobieganie nieautoryzowanym uzyskaniem dostępu przez użytkowników za pośrednictwem sieci, takiej jak internet. Zapora sieciowa może być aktywowana na danym połączeniu sieciowym. Aby włączyć zapory dla połączenia sieciowego, zaznacz pole wyboru „Włączony". Aby dowiedzieć się jak najwięcej na temat zabezpieczeń bramy, patrz punkt 5.2.



Rysunek 6.132 Zapora połączenia internetowego

Internetowe połączenie FastPath - zaznaczenie tego pola wyboru pozwala wykorzystać algorytm FastPath dla zwiększenia przepływu pakietów, co skutkuje szybszą komunikacją pomiędzy siecią LAN i WAN. Domyślnie ta funkcja jest włączona.

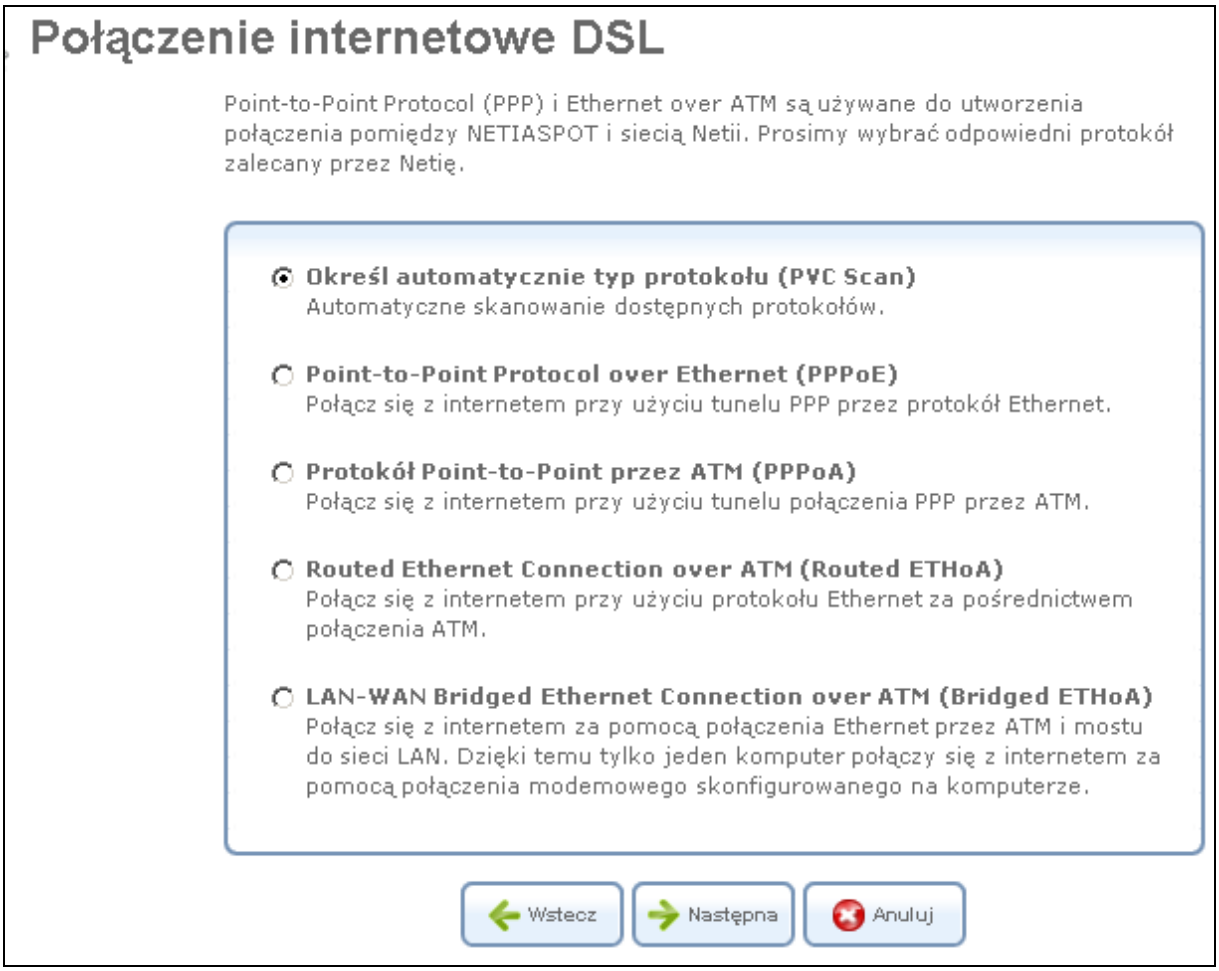


Rysunek 6.133 Internetowe połączenie FastPath

6.4.11. Konfiguracja połączenia PPPoA

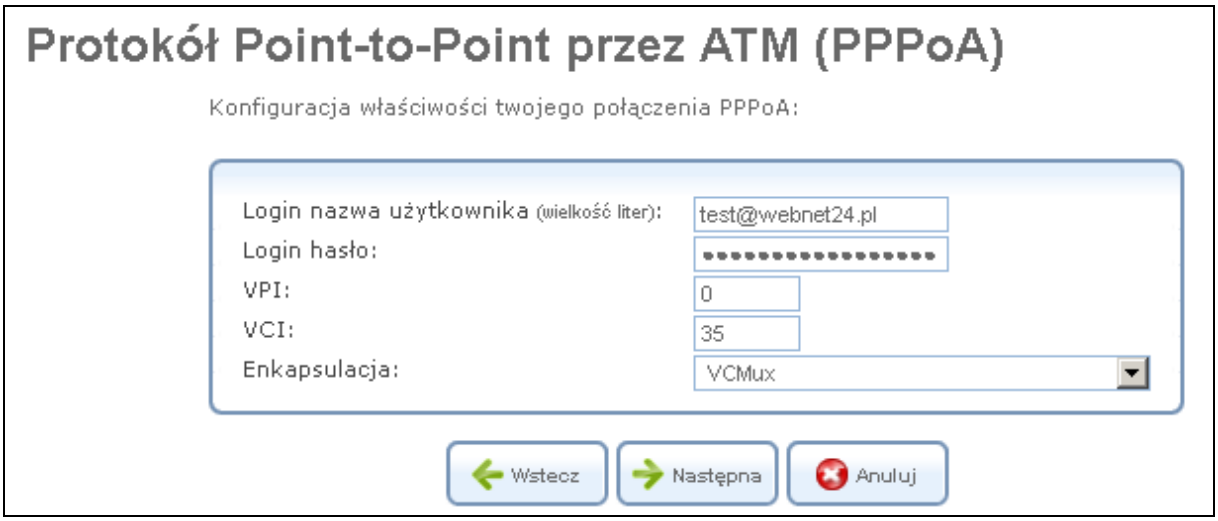
Aby utworzyć nowe połączenie PPPoA, wykonaj następujące czynności:

1. Kliknij przycisk „Nowe połączenie" link w sekcji „Połączenia sieciowe". Wyświetlony zostanie ekran kreatora połączeń (patrz rysunek 6.18).
2. Wybierz „Połączenie z internetem DSL", a następnie przycisk „Dalej" (patrz rysunek 6.19).
3. Wybierz „Point-to-Point Protocol przez ATM (PPPoA)", a następnie kliknij przycisk „Dalej". Zostaną wyświetlone parametry konfiguracji DSL PVC.



Rysunek 6.134 DSL PVC Parametry konfiguracji

4. Jeśli chcesz uzyskać parametry PVC automatycznie, wybierz „Automatyczne skanowanie PVC", a następnie kliknij przycisk „Dalej". W rozdziale 6.4.9 uzyskamy więcej informacji. W przeciwnym razie, możemy wybrać przycisk „Ustawienia ręczne PVC", a następnie kliknąć przycisk „Dalej". Wyświetlony zostanie ekran „Point-to-Point Protocol przez ATM (PPPoA)".

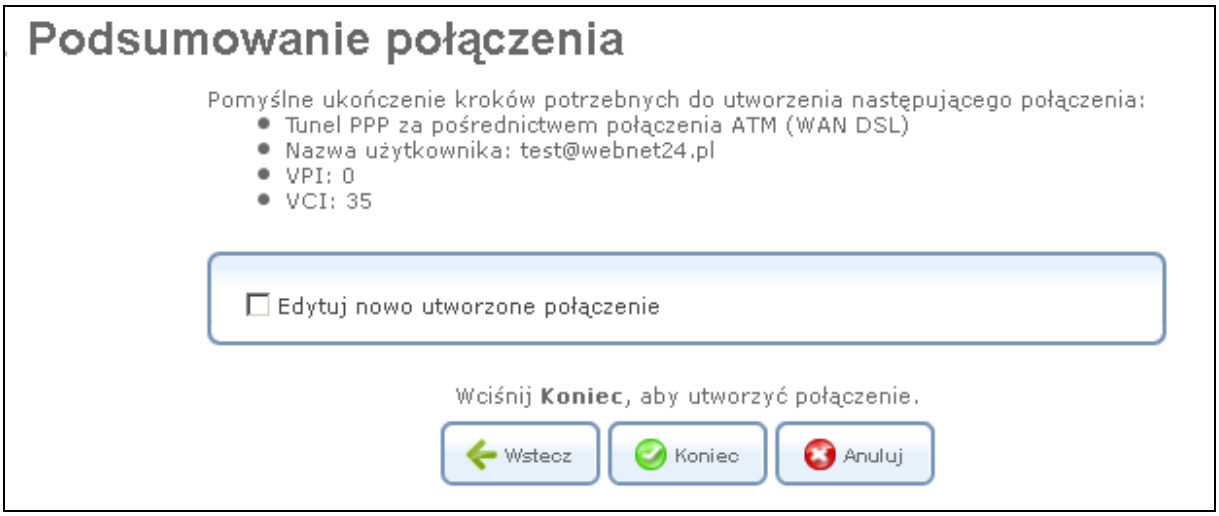


Rysunek 6.135 Point-to-Point Protocol przez ATM

5. Wprowadź nazwę użytkownika i hasło, które powinny być dostarczane przez operatora „Internet Sernice Provider" (ISP). Jeśli wybierzemy ręczne skanowanie

PVC w poprzednim kroku, należy wprowadzić następujące parametry, a także: identyfikator pary VPI i VCI i metodę enkapsulacji: LLC, VCMux lub VCMux HDLC.

6. Kliknij przycisk „Dalej”. Wyświetlony zostanie ekran „Podsumowanie połączenia”.



Rysunek 6.136 Podsumowanie połączenia

7. Wybierz pole wyboru „Edytuj nowo utworzone połączenie”, jeśli nie chcesz zostać skierowany na nowy ekran konfiguracji połączenia po kliknięciu „Koniec”. Ekran ten jest opisany w dalszej części tego rozdziału.
8. Kliknij przycisk „Zakończ”, aby zapisać ustawienia.

Nowe połączenie PPPoA zostanie dodane do listy połączeń sieciowych i będzie konfigurowalne jak każde inne połączenie.

6.4.11.1 Przeglądanie i edytowanie ustawień połączenia.

Aby wyświetlić i zmienić ustawienia połączenia PPPoA, należy kliknąć link „WAN PPPoA” w ekranie „Połączenia sieciowe”. Wyświetlony zostanie ekran „Właściwości WAN PPPoA”.

Rysunek 6.137 Właściwości połączenia WAN PPPoA

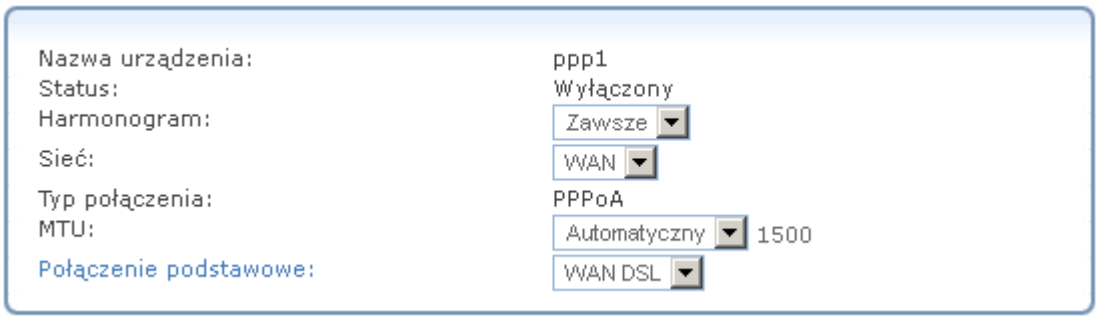
6.4.11.1.1 Ogólne

Ta sekcja umożliwia wyświetlanie ustawień połączenia PPPoA. Wprowadzone ustawienia mogą być edytowane w pozostałej sekcji interfejsu, jak opisano w następujących sekcjach.

6.4.11.1.2 Ustawienia

Sekcja „Ustawienia" pozwala modyfikować następujące ustawienia PPPoA:

Ogólne - ta sekcja wyświetla ogólne parametry połączenia.



Rysunek 6.138 Ogólne ustawienia PPPoA

Harmonogram - domyślnie połączenie jest zawsze aktywne. Jednakże, można skonfigurować zasady harmonogramu w celu określenia segmentów czasu, w którym połączenie może być aktywne. Po wybraniu zdefiniowanej reguły, z rozwijanego menu

pozwala na wybór pomiędzy dostępnymi regułami. Aby dowiedzieć się, jak skonfigurować reguły harmonogramu, możemy odnieść się do „Definiowania reguł harmonogramu" w części administracyjnej instrukcji OpenRG.

Sieć - wybierz, czy parametry konfigurowane odnoszą się do połączenia WAN, LAN lub DMZ wybierając typ połączenia z rozwijanego menu. Aby uzyskać więcej informacji, odnoszących się do powyższej funkcji, możemy ich znaleźć w sekcji „Typy sieci" administracyjnej instrukcji OpenRG. Należy pamiętać, że przy definiowaniu połączenia sieci jako DMZ, należy także:

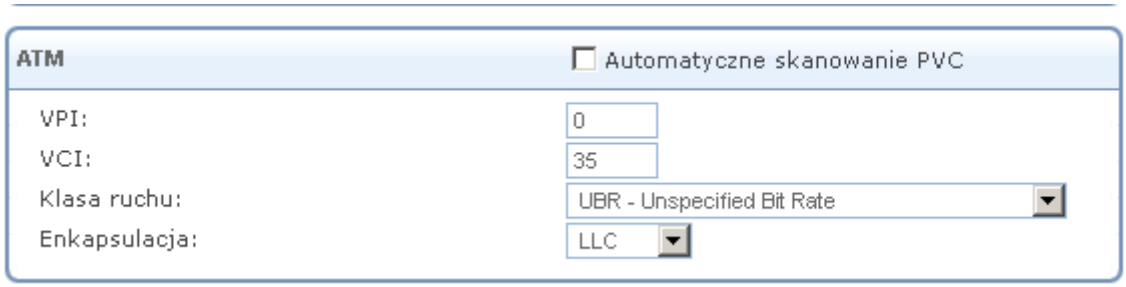
• Odłączyć połączenie z mostu, jeśli takie istnieje.
• Zmiana trybu połączenia trasy do „Router", w „Routingu".
• Dodaj reguły routingu na zewnątrz bramy (które mogą być dostarczane przez ISP), informuj sieć DMZ za OpenRG.

MTU - MTU jest to maksymalna jednostka transmisji. Określa ona największy rozmiar pakietu, jakim możemy przekazywać dane do Internetu. W ustawieniach domyślnych, automatycznie brama wybiera najlepsze MTU dla połączenia internetowego. Wybierz opcję „Automatycznie przez serwer DHCP", wtedy DHCP określenia wielkość MTU. W przypadku wybrania opcji „Ręcznie" zaleca się wpisać wartość od 1200 do 1500.

Połączenie bazowe - określa podstawowe połączenia, powyżej którego protokół będzie zainicjowany.

ATM - Asynchronous Transfer Mode (ATM) to technologia oparta na przesyłania danych w sieciach komórkowych lub pakietów o stałej wielkości. Używane komórki ATM są stosunkowo niewielkie w porównaniu do jednostek używanych w innych technologiach. Mała, stała wielkość komórek pozwala na transmisję wideo, audio i danych komputerowych, zapewniając, że żaden pojedynczy typ danych nie zużyje połączenia. Adresowanie ATM składa się z dwóch identyfikatorów, które określają ścieżkę wirtualną (VPI) i wirtualne połączenie (VCI). Ścieżka wirtualna składa się z wielu kanałów wirtualnych do tego samego punktu końcowego. Enkapsulacja do połączenia powinna być ustawiona

jako „LLC" lub „VCMux". Należy skonfigurować te parametry zgodnie z informacjami przekazanymi przez ISP.



Rysunek 6.139 Ustawienia ATM

Protokół internetowy - wybierz jedną z następujących opcji protokołu internetowego

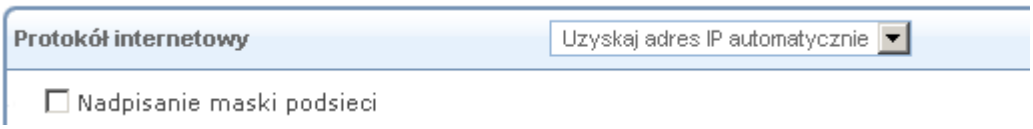
• Nienumerowany

• Uzyskaj adres IP automatycznie

• Użyj następującego adresu IP

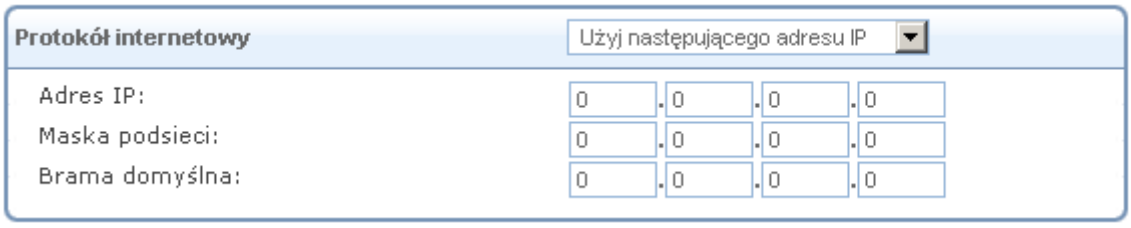
Zwróć uwagę, że ekran zostanie odświeżony, aby wyświetlić odpowiednie ustawienia zgodnie z Twoim wyborem.

Uzyskaj adres IP automatycznie - połączenie jest domyślnie skonfigurowane do pracy jako klient DHCP. Należy zachować tą konfigurację w przypadku, gdy usługodawca obsługuje DHCP lub jeśli łączysz się za pomocą dynamicznego adresu IP. Serwer operatora, przypisuje parametry bramy adresem IP i wyznacza maskę podsieci. Możesz zmienić dynamiczną maskę podsieci przypisaną przez DHCP, wybierając opcję „Zastąp maskę podsieci" i określ własną maskę zamiast przypisanej. Można kliknąć przycisk „Zwolnij", aby zwolnić bieżącą dzierżawę adresu IP. Po kliknięciu „Zwolnij" adres został zwolniony, należy kliknąć „Odnów". Użyj przycisku „Odnów" odnowienia dzierżawę adresu IP.



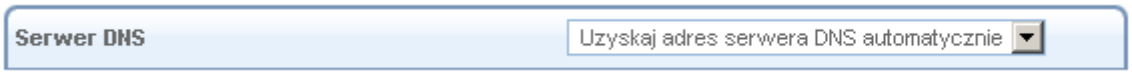
Rysunek 6.140 Automatyczne uzyskiwanie parametrów interfejsu

Użyj następującego adresu IP - połączenie można skonfigurować za pomocą stałego (statycznego) adresu IP. Usługodawca powinien zapewnić wtedy taki adresu IP i maskę podsieci.



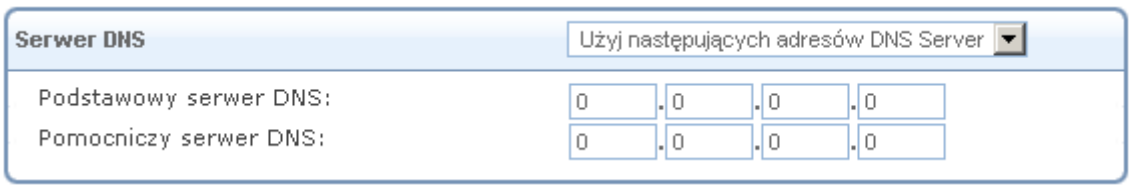
Rysunek 6.141 Protokół internetowy – Statyczne IP

Serwer DNS - Domain Name System (DNS) jest metodą, w której nazwy domeny witryny sieci www, są tłumaczone na adresy IP. Możesz skonfigurować połączenie do automatycznego uzyskania adresów serwera DNS, albo określić takiego adresy ręcznie, zgodnie z informacjami dostarczanymi przez ISP. Aby skonfigurować połączenie do automatycznego uzyskania serwera DNS, wybierz opcję „Uzyskaj adres serwera DNS automatycznie" z rozwijanego menu „Serwer DNS".



Rysunek 6.142 Serwer DNS – Automatyczne uzyskiwanie parametrów

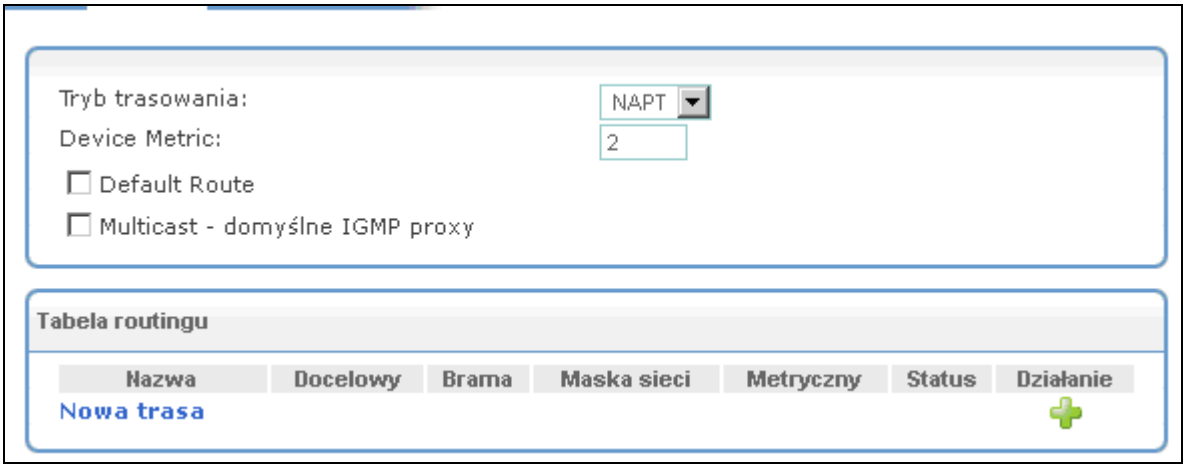
Aby ręcznie skonfigurować adresy serwerów DNS, wybierz opcję „Użyj następujących serwerów DNS" z rozwijanego menu (patrz rysunek „Serwer DNS - Statyczne IP"). Określ do dwóch różnych adresów serwera DNS, pierwotny i zapasowy.



Rysunek 6.143 Serwer DNS - Statyczne IP

6.4.11.1.3 Trasowanie

Ta zakładka umożliwia skonfigurowanie ustawień trasowania połączenia. Można wybrać i skonfigurować bramę do statycznego lub dynamicznego routingu. Routing dynamiczny automatycznie dostosowuje tablice trasowania do ruchu pakietów w sieci. Routing statyczny określa stałą ścieżkę do innych podsieci.



Rysunek 6.144 Zaawansowane właściwości trasowania

Możesz skonfigurować następujące ustawienia:

Tryb trasowania - wybierz jeden z następujących trybów trasy:

Trasa - użyj tej funkcji, jeśli chcesz , aby brama działania jako router między dwoma sieciami.

NAPT - Network Address Port Translation (NAPT) odnosi się do procesu translacji adresów z udziałem mapowania numerów portów, dzięki czemu wiele maszyn przy posiadaniu jednego publicznego adresu IP. Użyj NAPT, jeśli LAN obejmuje wiele urządzeń, topologii, które wymagają tłumaczenia port oprócz translacji adresów.

Device metric (metryka urządzenia) - jest wartością używaną przez bramę w celu określenia, czy jedna trasa jest lepsza od innej, biorąc pod uwagę takie parametry jak przepustowość, opóźnienie i wiele innych.

Trasa domyślna - zaznacz to pole wyboru w celu określenia tego urządzenia jako domyślnej trasy.

Multicast - domyślne proxy IGMP - OpenRG służy jako serwer proxy IGMP, wydawanie przyjmowanych komunikatów IGMP w imieniu podłączonych komputerów z sieci lokalnej. To pole wyboru jest aktywne domyślnie w sieci LAN, co oznacza, że jeśli serwer multicast jest dostępny w LAN, inne komputery z sieci LAN wyślą prośbę, aby dołączyć do grup multicast (wyślą żądanie IGMP). Jednak to pole wyboru jest wyłączone domyślnie dla połączenia WAN, co oznacza, że komputery z sieci lokalnej nie będą w stanie dołączyć do grupy multicast WAN serwerów multicast. Podczas tworzenia mostu sieciowego WAN-LAN, to pole wyboru musi być odznaczone.

Wersja IGMP Query - OpenRG obsługuje wszystkie trzy wersje IGMP. Wybierz wersję, której chcesz użyć. Pamiętaj, że menu rozwijane pojawia się tylko podczas połączenia LAN.

Tabela routingu - umożliwia dodanie lub zmianę trasy, gdy urządzenie jest aktywne. Użyj przycisku „Nowa trasa", aby dodać trasy lub edytować istniejące trasy.

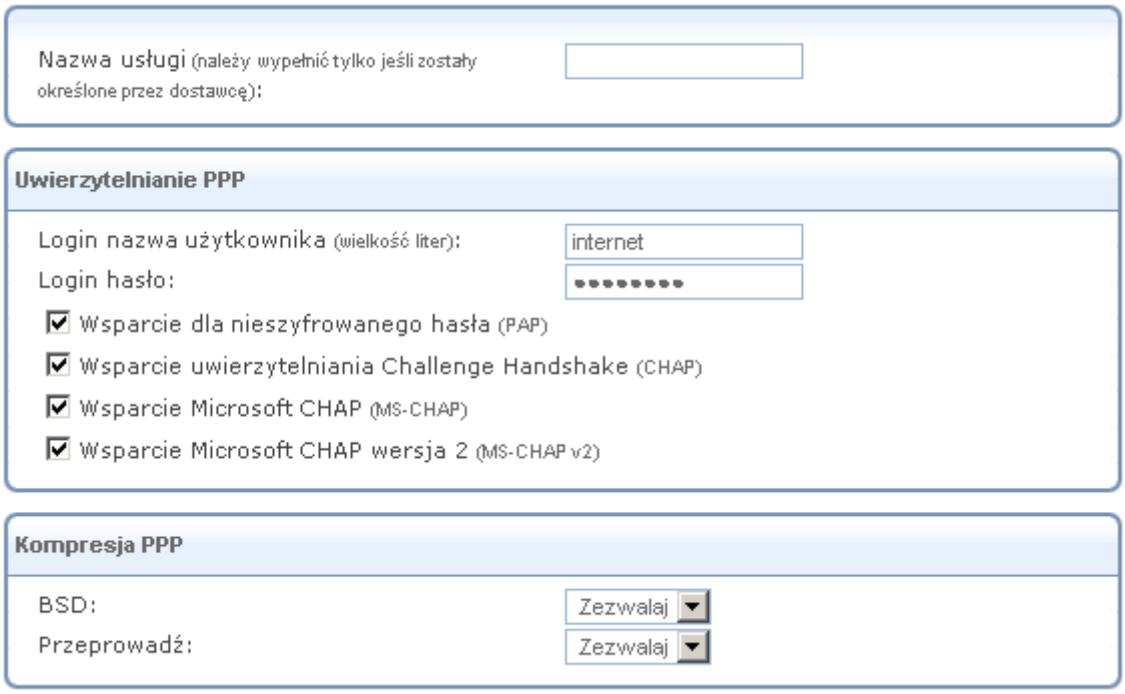
6.4.11.1.4 PPP

Point-to-Point Protocol (PPP) jest najbardziej popularną metodą transportu pakietów pomiędzy użytkownikiem a dostawcą usług internetowych. PPP obsługuje protokoły uwierzytelniania, takie jak PAP i CHAP, jak również inne, takie jak kompresje i protokoły szyfrowania.

PPP na żądanie – opcja PPP na żądanie rozpoczyna sesję punkt-punkt tylko gdy pakiety są rzeczywiście wysyłane przez internet.

Rysunek 6.145 Konfiguracja PPP na żądanie

Czas między próbami ponownego połączenia – należy podać czas trwania między ponownym połączeniem PPP, dane jeśli będą wymagane to zostaną dostarczone przez ISP.



Uwierzytelnianie PPP - Point-to-Point Protocol (PPP), obecnie obsługuje cztery protokoły uwierzytelniania: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) i Microsoft CHAP w wersji 1 i 2. Ta sekcja pozwala na wybranie protokołu uwierzytelniania bramy. Wybrany protokół mogą wykorzystać podczas negocjacji z serwerem PPTP. Wybierz wszystkie protokoły, jeśli nie ma dostępnych informacji na temat serwera protokołu uwierzytelniania. Uwaga - szyfrowanie odbywa się tylko wtedy, gdy wybrane są Microsoft CHAP, Microsoft CHAP wersja 2, albo zostały wybrane oba.

Rysunek 6.146 Uwierzytelnianie PPP

Login Nazwa użytkownika zgodnie z ustaleniami z ISP.

Login Hasło - zgodnie z ustaleniami z ISP.

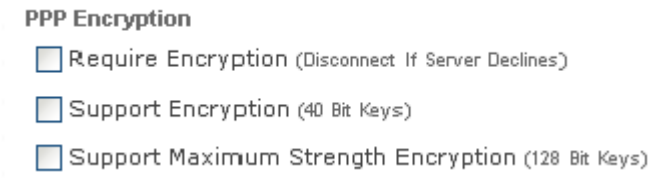
Wsparcie niezaszyfrowanego hasła (PAP) - protokół uwierzytelniania hasła (PAP) jest prosty, schematu uwierzytelniania odbywa się zwykłym tekstem. Nazwa użytkownika i hasło są wysyłane przez sieć w postaci zwykłego tekstu. PAP nie jest bezpiecznym protokołem uwierzytelniania.

Challenge Authentication Support Handshake (CHAP) – jest to protokół uwierzytelniania typu wyzwanie-odpowiedź, który używa hash MD5 do zabezpieczenia odpowiedzi na zapytanie. CHAP jest bezpiecznym protokołem uwierzytelniania, zapewnia ochronę przed atakami wykorzystującymi podsłuch transmisji, wykorzystuje MD5. Jest preferowany jako uwierzytelnianie w PPP.

Wsparcie Microsoft CHAP - zaznacz to pole wyboru, jeśli komunikujesz się z użytkownikami, którzy używają protokołu uwierzytelniania CHAP Microsoft.

Wsparcie Microsoft CHAP w wersji 2 - zaznacz to pole wyboru, jeśli komunikujesz się z użytkownikami, którzy używają protokołu uwierzytelniania Microsoft CHAP w wersji 2.

Szyfrowanie PPP - PPP obsługuje szyfrowanie w celu zabezpieczenia danych połączenia w sieci. Szeroki wybór metod szyfrowania może być negocjowany, choć zwykle tylko jedna metoda jest stosowana do każdego kierunku połączenia. Ta sekcja pozwala na wybranie metod szyfrowania używanych przez bramę, które mogą być wykorzystane podczas negocjacji z serwerem PPTP. Wybierz wszystkie metody, jeżeli nie posiadamy informacji na temat metody szyfrowania używanego przez serwer. Proszę pamiętać, że szyfrowanie PPP może być używane tylko z protokołem uwierzytelniania MS-CHAP lub MS-CHAP-V2.



Rysunek 6.147 Szyfrowanie PPP

Wymagaj szyfrowania - zaznaczamy to pola wyboru, aby zapewnić, że połączenie PPP jest szyfrowane.

Obsługa szyfrowania (40 bitowe klucze) - zaznaczamy to pole wyboru, jeśli użytkownik obsługuje 40-bitowe klucze szyfrowania.

Wsparcie maksymalnej siły szyfrowania (128 bitowych kluczy) - zaznaczamy to pole wyboru, jeśli użytkownik obsługuje 128 bitowe klucze szyfrowania.

Kompresja PPP – „Compression Control Protocol" (CCP) jest odpowiedzialny za konfigurację, dzięki czemu umożliwiają włączenie/wyłączenie algorytmów kompresji na obu końcach połączenia punkt-punkt. Jest również używany jako mechanizm sygnalizacji awarii kompresji/dekompresji w wiarygodny sposób.

Rysunek 6.148 Kompresja PPP

Dla każdego algorytmu kompresji, wybierz jedną z następujących opcji z menu rozwijanego:

Odrzuć - odrzucenie połączeń PPP z użytkownikami, którzy korzystają z algorytmu kompresji.

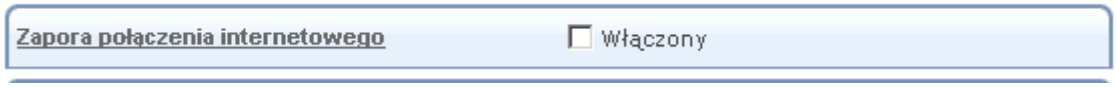
Zezwalaj - zezwalaj na połączenia PPP z użytkownikami, którzy korzystają z algorytmu kompresji.

Wymagaj - zapewniaj połączenie PPP z użytkownikami, którzy korzystają z algorytmu kompresji.

6.4.11.1.5 Zaawansowane

Ta sekcja pozwala skonfigurować ustawienia zaawansowane interfejsu PPPoA.

• **Zapora połączenia internetowego** - Twoja zapora sieciowa urządzenia pomaga chronić komputer poprzez zapobieganie nieautoryzowanym uzyskaniem dostępu przez użytkowników za pośrednictwem sieci, takiej jak Internet. Zapora sieciowa może być aktywowana na danym połączeniu sieciowym. Aby włączyć zapory dla połączenia sieciowego, zaznacz pole wyboru „Włączony". Aby dowiedzieć się jak najwięcej na temat zabezpieczeń bramy, patrz punkt 5.2.



Rysunek 6.149 Zapora połączenia internetowego

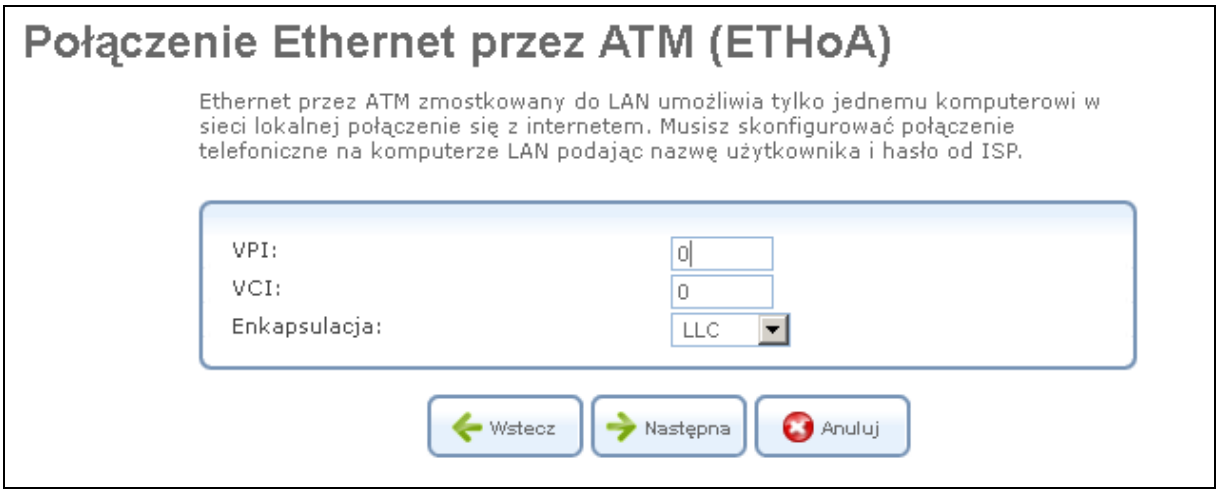
6.4.12. Konfiguracja połączenia ETHoA

Połączenie Ethernet przez ATM (ETHoA) umożliwia transport ramek Ethernet przez łącze DSL.

6.4.12.1 Tworzenia połączenia ETHoA

Podczas tworzenia połączenia ETHoA przez funkcję „Połącz z Internetem DSL" dane zostaną przesłane mostem sieciowym do LAN. Musisz skonfigurować połączenie telefoniczne na komputerze użytkownika LAN z danymi od dostawcy usługi, takimi jak nazwa i hasło. Aby utworzyć nowe połączenie ETHoA, wykonaj następujące czynności:

1. Kliknij przycisk „Nowe połączenie” link w sekcji „Połączenia sieciowe”. Wyświetlony zostanie ekran kreatora połączeń (patrz rysunek 6.18).
2. Wybierz „Połącz z Internetem DSL”, a następnie przycisk „Dalej” (patrz rysunek 6.19).
3. Wybierz „Połączenie Ethernet przez ATM (ETHoA)”, a następnie przycisk „Dalej”. Wyświetlony zostanie ekran „Połączenie Ethernet przez ATM (ETHoA)”.



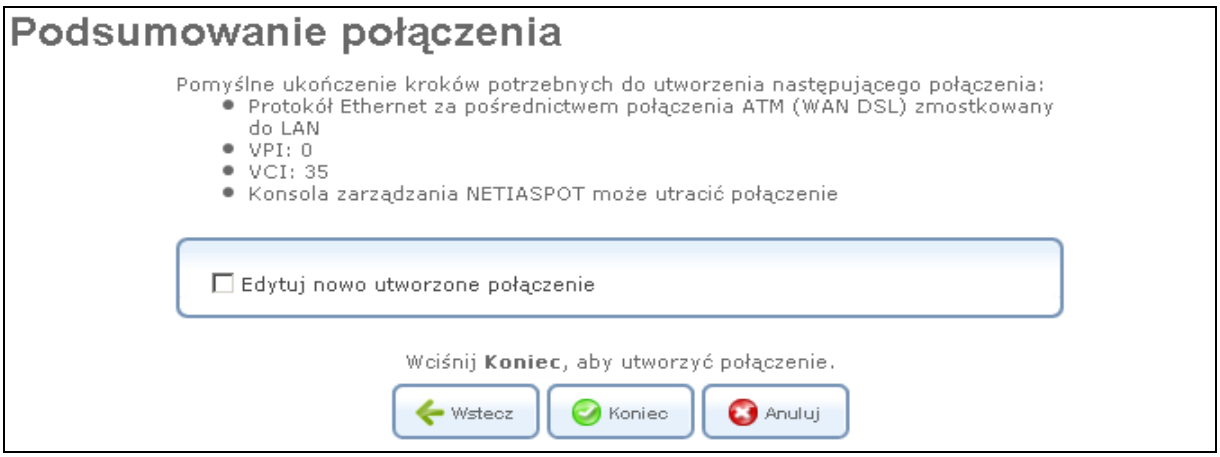
Rysunek 6.150 Połączenie Ethernet przez ATM

4. Wprowadź następujące informacje, które powinny być dostarczane przez (ISP):

• Identyfikator pary VPI i VCI.

• Sposób enkapsulacji: LLC lub VCMux.

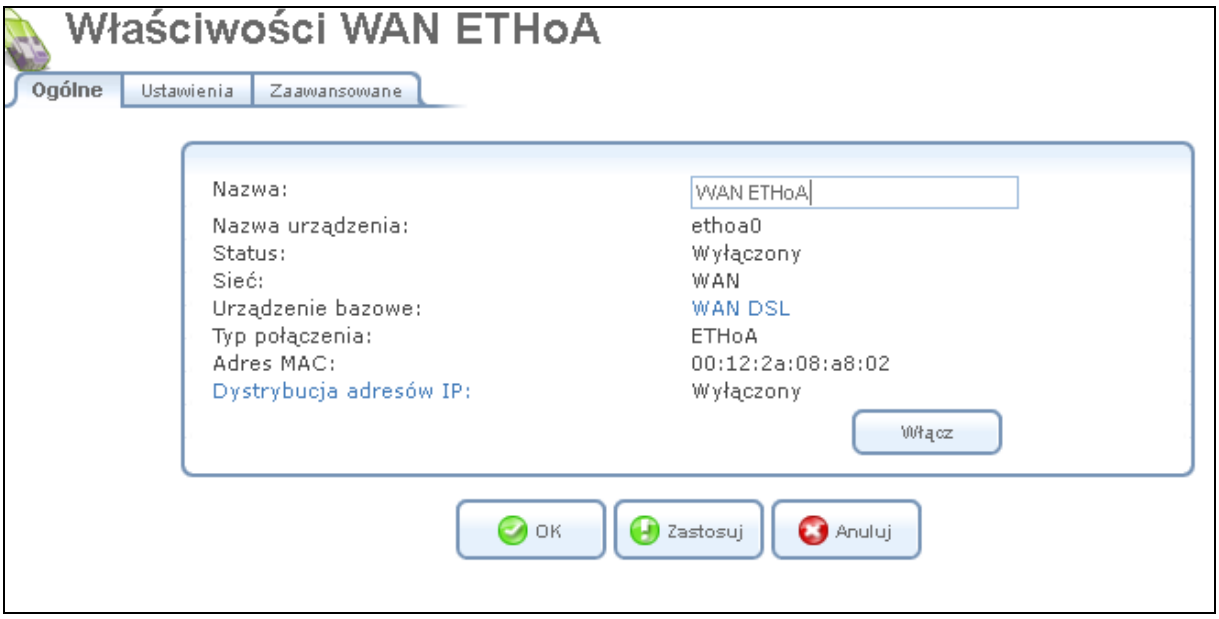
5. Kliknij przycisk „Dalej”. Wyświetlony zostanie ekran „Podsumowanie połączenia”.



Rysunek 6.151 podsumowanie połączenia

6. Wybierz pole wyboru „Edytuj nowo utworzone połączenie", jeśli chcesz być skierowany do nowego ekranu konfiguracji połączenia po kliknięciu „Koniec". Ekran ten jest opisany w dalszej części rozdziału.
7. Kliknij przycisk „Zakończ", aby zapisać ustawienia.

Nowe połączenie ETHoA zostanie dodane do listy połączeń sieciowych i będzie konfigurowalne jak każde inne połączenie.



Rysunek 6.152 Właściwości połączenia WAN ETHoA

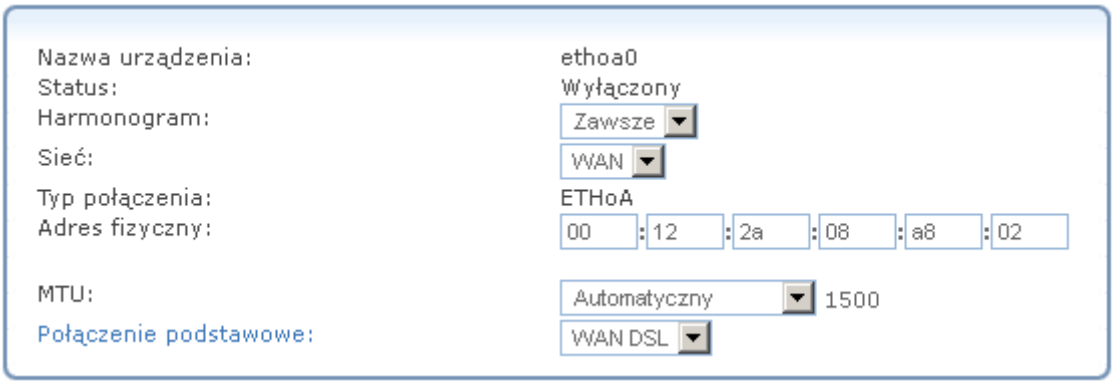
6.4.12.1.1 Ogólne

Ta sekcja umożliwia wyświetlanie ustawień połączenia ETHoA (patrz rys. 6.120). Wprowadzone ustawienia mogą być edytowane w pozostałej sekcji interfejsu, jak opisano w następujących sekcjach.

6.4.12.1.2 Ustawienia

Sekcja „Ustawienia" pozwala modyfikować następujące ustawienia ETHoA:

Ogólne - ta sekcja wyświetla ogólne parametry połączenia.



Rysunek 6.153 Ogólne ustawienia ETHoA

Harmonogram - domyślnie połączenie jest zawsze aktywne. Jednakże, można skonfigurować zasady harmonogramu w celu określenia segmentów czasu, w którym połączenie może być aktywne. Po wybraniu zdefiniowanej reguły, z rozwijanego menu pozwala na wybór pomiędzy dostępnymi regułami. Aby dowiedzieć się, jak skonfigurować reguły harmonogramu, możemy odnieść się do „Definiowania reguł harmonogramu" w części administracyjnej instrukcji OpenRG.

Sieć - wybierz, czy parametry konfigurowane odnoszą się do połączenia WAN, LAN lub DMZ wybierając typ połączenia z rozwijanego menu. Aby uzyskać więcej informacji, odnoszących się do powyższej funkcji, możemy ich znaleźć w sekcji „Typy sieci" administracyjnej instrukcji OpenRG. Należy pamiętać, że przy definiowaniu połączenia sieci jako DMZ, należy także:

• Odłączyć połączenie z mostu, jeśli takie istnieje.
• Zmiana trybu połączenia trasy do „Router", w „Routingu".
• Dodaj reguły routingu na zewnątrz bramy (które mogą być dostarczane przez ISP), informuj sieć DMZ za OpenRG.

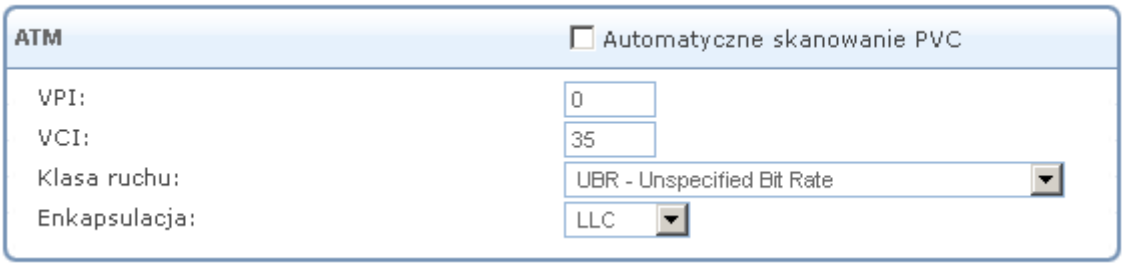
Adres fizyczny – pole adresu fizycznego MAC interfejsu sieciowego. Niektóre interfejsy pozwalają na zmianę wartości adresu MAC.

Klonuj mój adres MAC - naciśnij ten przycisk, aby skopiować aktualny adres MAC z karty sieciowej komputera.

MTU - MTU jest to maksymalna jednostka transmisji. Określa ona największy rozmiar pakietu, jakim możemy przekazywać dane do Internetu. W ustawieniach domyślnych, automatycznie brama wybiera najlepsze MTU dla połączenia internetowego. Wybierz opcję „Automatycznie przez serwer DHCP", wtedy DHCP określenia wielkość MTU. W przypadku wybrania opcji „Ręcznie" zaleca się wpisać wartość od 1200 do 1500.

Połączenie bazowe - określa podstawowe połączenia, powyżej którego protokół będzie zainicjowany.

ATM - Asynchronous Transfer Mode (ATM) to technologia oparta na przesyłania danych w sieciach komórkowych lub pakietów o stałej wielkości. Używane komórki ATM są stosunkowo niewielkie w porównaniu do jednostek używanych w innych technologiach. Mała, stała wielkość komórek pozwala na transmisję wideo, audio i danych komputerowych, zapewniając, że żaden pojedynczy typ danych nie zużyje połączenia. Adresowanie ATM składa się z dwóch identyfikatorów, które określają ścieżkę wirtualną (VPI) i wirtualne połączenie (VCI). Ścieżka wirtualna składa się z wielu kanałów wirtualnych do tego samego punktu końcowego. Enkapsulacja do połączenia powinna być ustawiona jako „LLC" lub „VCMux". Należy skonfigurować te parametry zgodnie z informacjami przekazanymi przez ISP.



Rysunek 6.154 Ustawienia ATM

Protokół internetowy - wybierz jedną z następujących opcji protokołu internetowego

• Nienumerowany

• Uzyskaj adres IP automatycznie

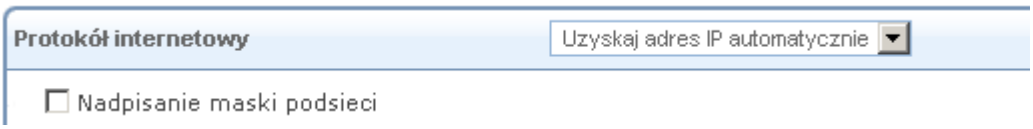
• Użyj następującego adresu IP

Zwróć uwagę, że ekran zostanie odświeżony, aby wyświetlić odpowiednie ustawienia zgodnie z Twoim wyborem.

Brak adresu IP - wybierz „Brak adresu IP", jeśli wymaga się, żeby brama nie posiadała adresu IP. Opcja ta może być użyteczna, jeśli pracujesz w środowisku, w które nie jest podłączone do innych sieci, takich jak internet.

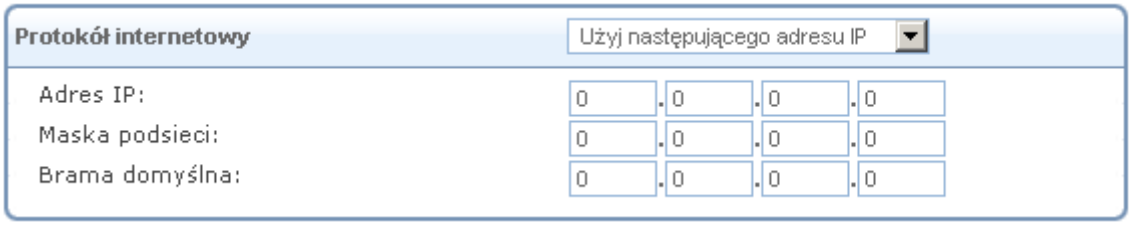
Rysunek 6.155 Protokół internetowy - Brak adresu IP

Uzyskaj adres IP automatycznie - połączenie jest domyślnie skonfigurowane do pracy jako klient DHCP. Należy zachować tą konfigurację w przypadku, gdy usługodawca obsługuje DHCP lub jeśli łączysz się za pomocą dynamicznego adresu IP. Serwer operatora, przypisuje parametry bramy adresem IP i wyznacza maskę podsieci. Możesz zmienić dynamiczną maskę podsieci przypisaną przez DHCP, wybierając opcję „Zastąp maskę podsieci" i określ własną maskę zamiast przypisanej. Można kliknąć przycisk „Zwolnij", aby zwolnić bieżącą dzierżawę adresu IP. Po kliknięciu „Zwolnij" adres został zwolniony, należy kliknąć „Odnów". Użyj przycisku „Odnów" odnowienia dzierżawę adresu IP.



Rysunek 6.156 Automatyczne uzyskiwanie parametrów interfejsu

Użyj następującego adresu IP - połączenie można skonfigurować za pomocą stałego (statycznego) adresu IP. Usługodawca powinien zapewnić wtedy taki adresu IP i maskę podsieci.

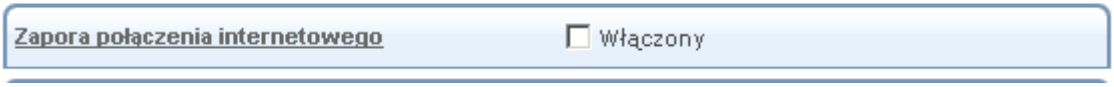


Rysunek 6.157 Protokół internetowy – Statyczne IP

6.4.12.1.3 Zaawansowane

Ta sekcja pozwala skonfigurować ustawienia zaawansowane interfejsu ETHoA.

• **Zapora połączenia internetowego** - Twoja zapora sieciowa urządzenia pomaga chronić komputer poprzez zapobieganie nieautoryzowanym uzyskaniem dostępu przez użytkowników za pośrednictwem sieci, takiej jak Internet. Zapora sieciowa może być aktywowana na danym połączeniu sieciowym. Aby włączyć zapory dla połączenia sieciowego, zaznacz pole wyboru „Włączony". Aby dowiedzieć się jak najwięcej na temat zabezpieczeń bramy, patrz punkt 5.2.



Rysunek 6.158 Zapora połączenia internetowego

• **Dodatkowe adresy IP** - można dodać aliasy (dodatkowe adresy IP) bramy, klikając na link „Nowy adres IP". Pozwala to dostępu do bramy za pomocą aliasów oprócz domyślnego 192.168.1.254 i http://netiaspot.home.

Rysunek 6.159 Dodatkowe adresy IP

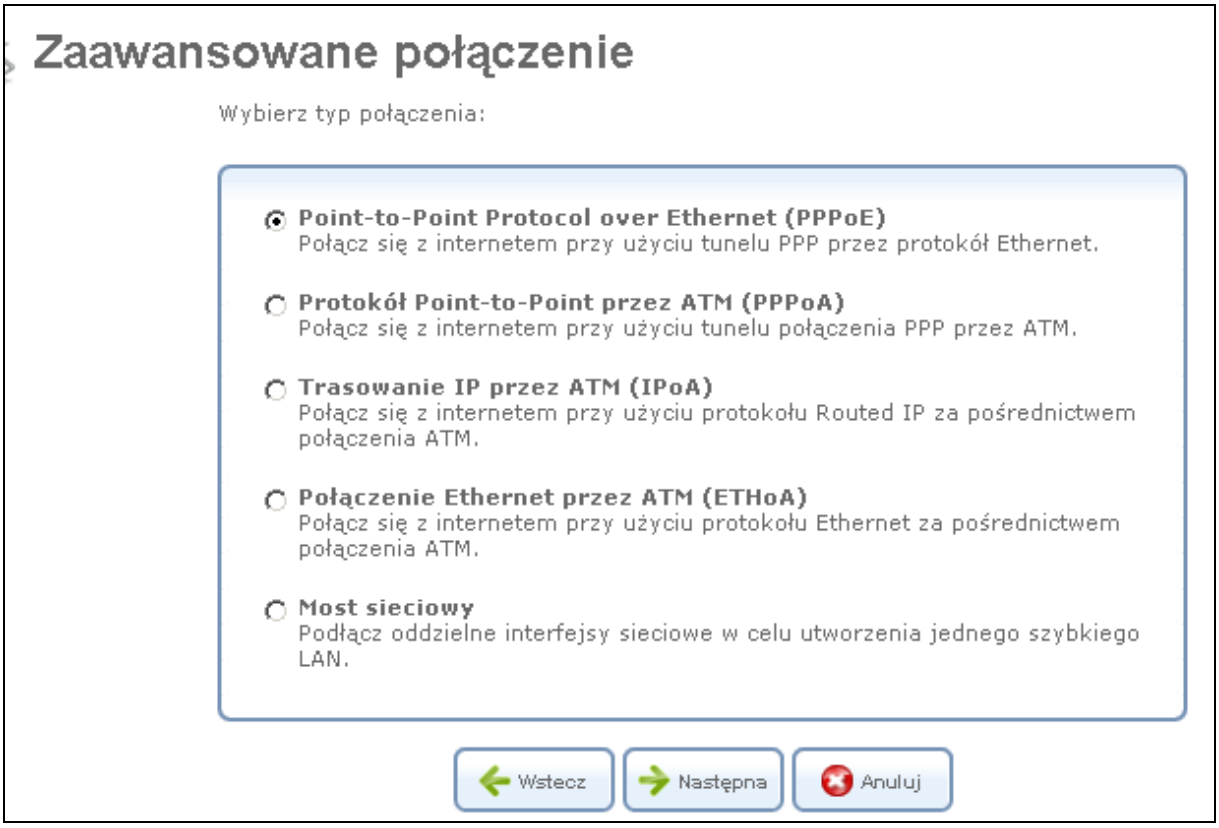
6.4.13 Konfiguracja mostu sieciowego WAN-LAN

Połączenie mostu sieciowego WAN-LAN mostkuje WAN i urządzenie w sieci LAN. W ten sposób komputer w sieci lokalnej OpenRG, może uzyskać adres IP, który jest adresem WAN.

6.4.13.1 Tworzenie połączenia motu sieciowegoWAN-LAN

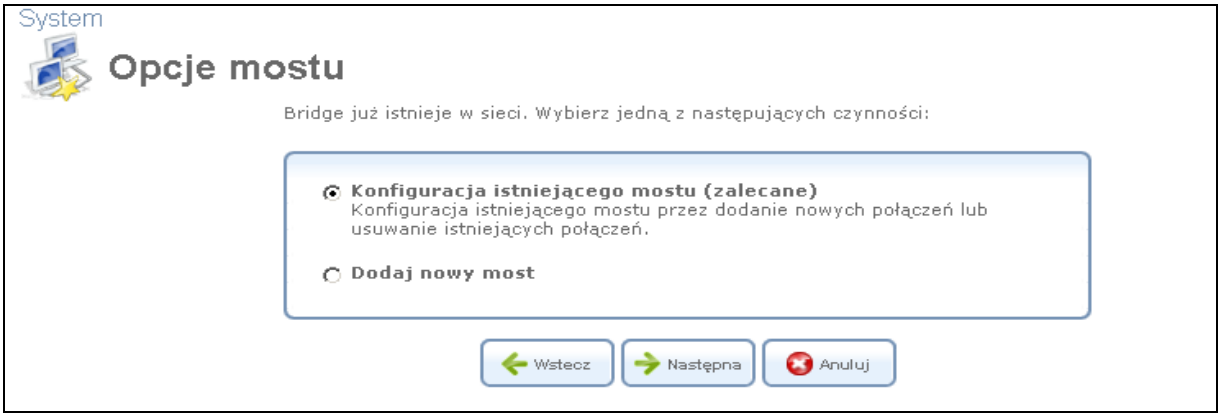
Aby utworzyć nowy most lub skonfigurować już istniejącego, wykonaj następujące czynności:

1. Na ekranie „Połączenia sieciowe" w sekcji „System" (patrz rysunek 6.10), kliknij „Nowe połączenie". Wyświetlony zostanie ekran kreatora połączenia (patrz rysunek 6.11, 6.18).
2. Wybierz opcję „Połączenie Zaawansowane", a następnie przycisk „Dalej". Wyświetlona zostanie sekcja „Połączenie zaawansowane".



Rysunek 6.160 Kreator zaawansowanego połączenia

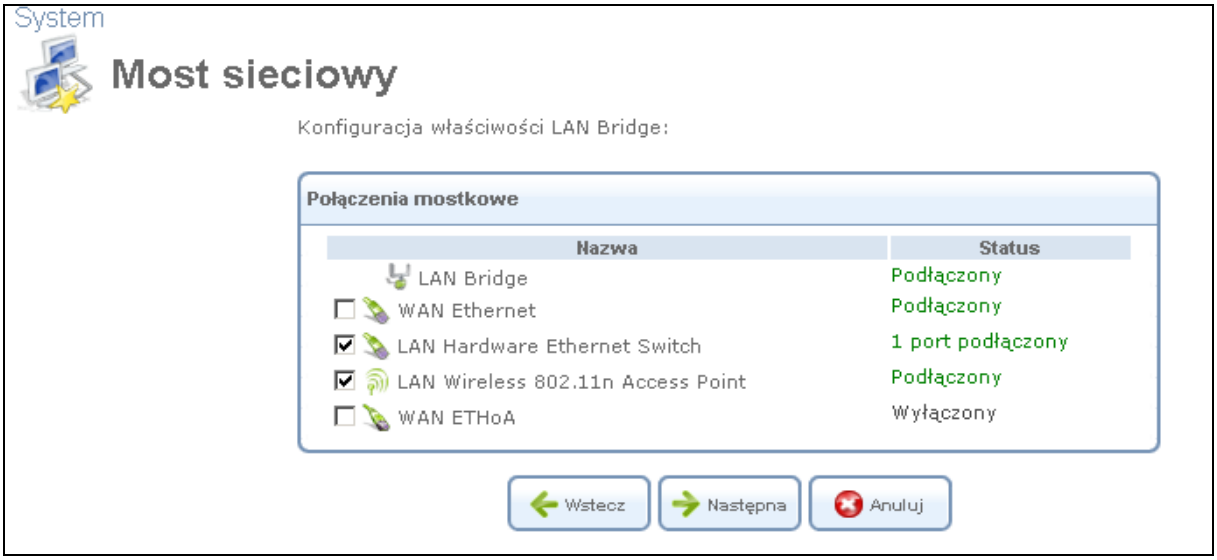
3. Wybierz przycisk „Most sieciowy", a następnie przycisk „Dalej". Wyświetlony zostanie ekran „Opcje mostu".



Rysunek 6.161 Opcje mostu

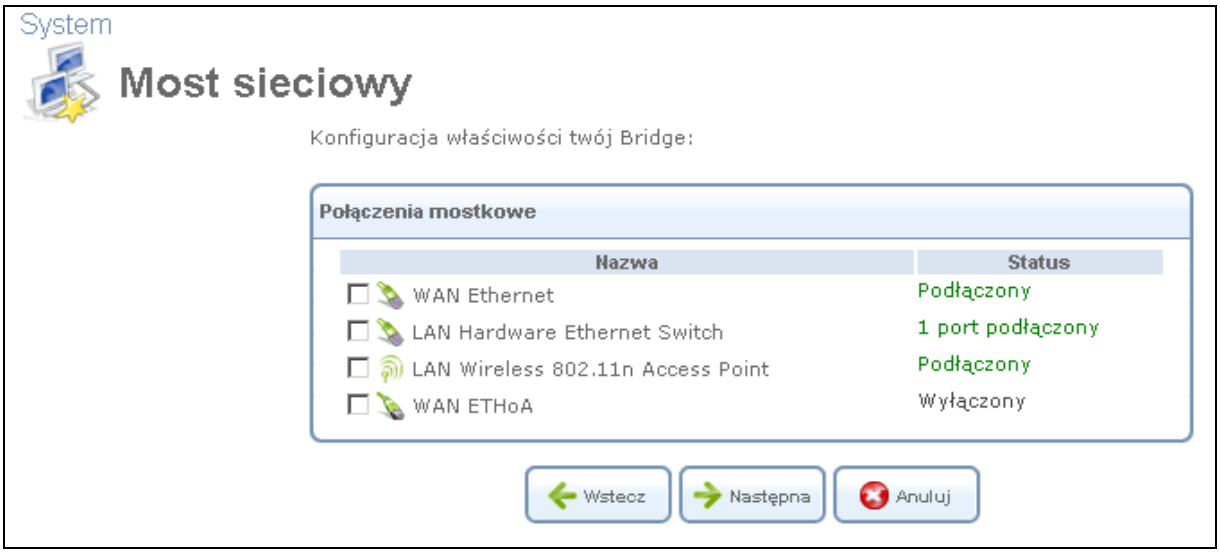
4. Wybierz, czy chcesz modyfikować konfigurację istniejącego mostu (ta opcja pojawi się tylko jeśli most istnieje) lub dodać nowy most:

a. **Konfiguracja istniejącego mostu** - wybierz tą opcję i kliknij „Dalej". Ekran „Most sieciowy" wyświetla aktualne połączone interfejsy i pozwala na dodawanie nowych połączeń do mostu lub pozwala usunąć istniejące przez ich zaznaczenie lub usuwając zaznaczenie pól wyboru. Na przykład, aby utworzyć most WAN-LAN, wybierz połączenie WAN z pola wyboru.



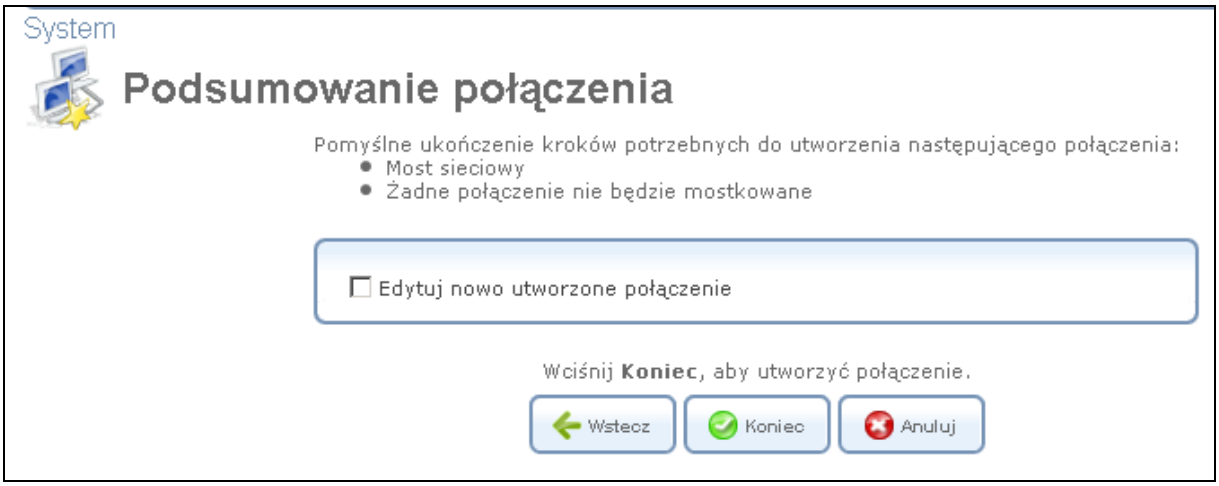
Rysunek 6.162 Most sieciowy – konfiguracja istniejącego mostu

b. Wybierz opcję „Dodaj nowy most sieciowy” i kliknij „Dalej”. W nowym oknie dialogowym zostaną wyświetlone możliwe do połączenia interfejsy sieciowe przez wybór odpowiednich pól wyboru.



Rysunek 6.163 Most sieciowy – dodanie nowego mostu sieciowego

5. Kliknij przycisk „Dalej”. Wyświetlony zostanie ekran „Podsumowanie połączenia”, wyświetlając odpowiednie zmiany.



Rysunek 6.164 Podsumowanie połączenia – konfiguracja istniejącego mostu

6. Wybierz pole wyboru „Edytuj nowo utworzone połączenie”, jeśli chcesz być skierowany do nowego ekranu konfiguracji połączenia po kliknięciu przycisku „Zakończ”. Ekran ten jest opisany w dalszej części tego rozdziału.

7. Kliknij przycisk "Zakończ ", aby zapisać ustawienia. Nowy most zostanie dodany do listy połączeń sieci i będzie konfigurowalny, jak każdy inny most.

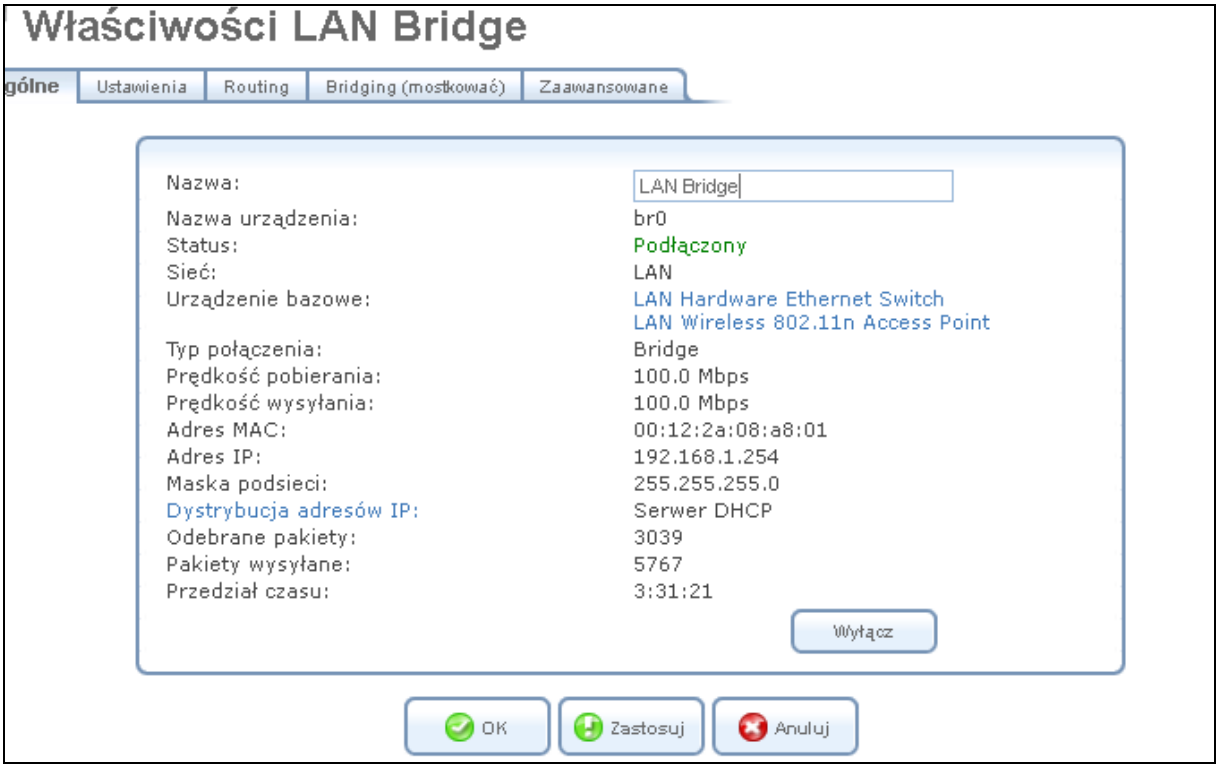
Nowy most zostanie dodany do listy połączeń sieciowych i będziemy mogli go konfigurować jak każdy inny most.

Uwaga: Utworzenie mostu sieciowego WAN-LAN wyłącza serwer DHCP OpenRG. Oznacza to, że komputery z sieci lokalnej mogą otrzymać adresu IP z serwera DHCP w sieci WAN. Jeśli skonfigurujemy hosta ze statycznym adresem IP z adresem podsieci mostu (192.168.1.x), będziemy mogli uzyskać dostęp do OpenRG, ale nie WAN, ponieważ NAT nie jest wykonywany w trybie mostu sieciowego WAN-LAN.

Po utworzeniu mostu sieciowego WAN-LAN, należy także wyłączyć IGMP proxy dla tego połączenia.

Aby to zrobić, wykonaj następujące czynności:

1. Na ekranie „Połączenia sieciowe" w sekcji „System", kliknij link „Most sieciowy LAN". Wyświetlone zostaną właściwości wybranego mostu sieciowego.



Rysunek 6.165 Właściwości mostu sieciowego

2. Wybierz zakładkę „Trasowanie” i wyłącz opcję „Multicast - IGMP Proxy”, która domyślnie jest włączona. Więcej informacji na temat tej opcji, patrz punkt 6.4.13.3.3.
3. Kliknij przycisk „OK”, aby zapisać ustawienia.

6.4.13.2 Włączanie trybu hybrydowego mostu sieciowego

OpenRG pozwala na przeniesienie określonego zapotrzebowania na pasmo i ruchu wrażliwego z komputerów w sieci lokalnej, takich jak IPTV Set Top Box, bezpośrednio do sieci WAN. Taki system połączenia z siecią nie koliduje z funkcją trasowania OpenRG, w której cały ruch zwykle przechodzi przez NAT i sprawdzany jest przez zaporę sieciową. Te dwa tryby mogą pracować jednocześnie, jeśli posiadamy dwa mosty sieciowe w LAN OpenRG:

Most sieciowy LAN - odbiera swój adres IP z serwera DHCP OpenRG. Ruch przechodzący za pośrednictwem sieci LAN w drodze do WAN jest kontrolowany przez zaporę sieciową OpenRG i przypisany zostanie mu publiczny adres przez NAT.

Most WAN-LAN - odbiera swój adres IP z serwera DHCP WAN, umożliwiając tym samym bezpośrednie połączenie z WAN.

OpenRG bazując na jądrze Linux 2.6 umożliwia bezpośrednią komunikację między dwoma mostami. Na przykład, jeśli połączysz urządzenie „IPTV Set Top Box” (STB) z „Personal Video Recorder” (PVR) do mostu sieciowego WAN-LAN OpenRG, będzie można uzyskać dostęp do treści nagranych na PVR z dowolnego komputera domowego podłączonego do sieci LAN OpenRG.

Ta konfiguracja sieci określana jest jako hybrydowy most sieciowy. OpenRG wykrywa komputery z sieci lokalnej, które powinny być połączone mostem z WAN według ich adresów MAC lub wybranej opcji DHCP (zarówno ID klasy producenta, ID klienta lub klasy ID użytkownika). Po wykryciu komputerów z sieci lokalnej znajdą się pod mostem

sieciowym WAN-LAN, który należy wcześniej dodać i skonfigurować w trybie hybrydowego mostu sieciowego.

Aby dodać most sieciowy WAN-LAN, wykonaj czynności opisane w kreatorze połączenia (rozdział 6.4.13.1). W ostatnim kroku należy sprawdzić zaznaczenie pola wyboru „Edytuj nowo utworzone połączenie" i kliknij przycisk „Zakończ". Zostanie wyświetlony ekran właściwości połączenia sieciowego.

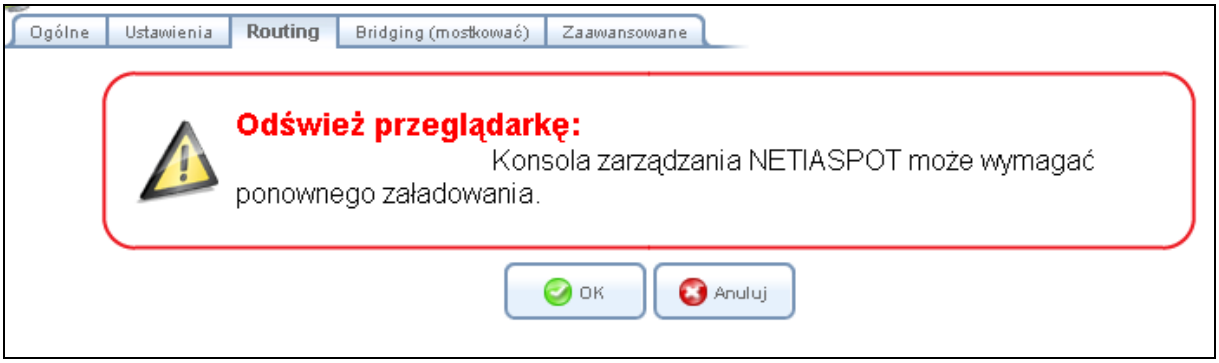
Rysunek 6.166 Właściwości mostu

Aby skonfigurować most sieciowy WAN-LAN w tryb mostu hybrydowego, wykonaj następujące czynności:

1. Na ekranie „Właściwości mostu sieciowego", kliknij zakładkę „Trasowanie". Pojawi się następujący ekran.

Rysunek 6.167 Most sieciowy WAN-LAN ustawienia trasowania

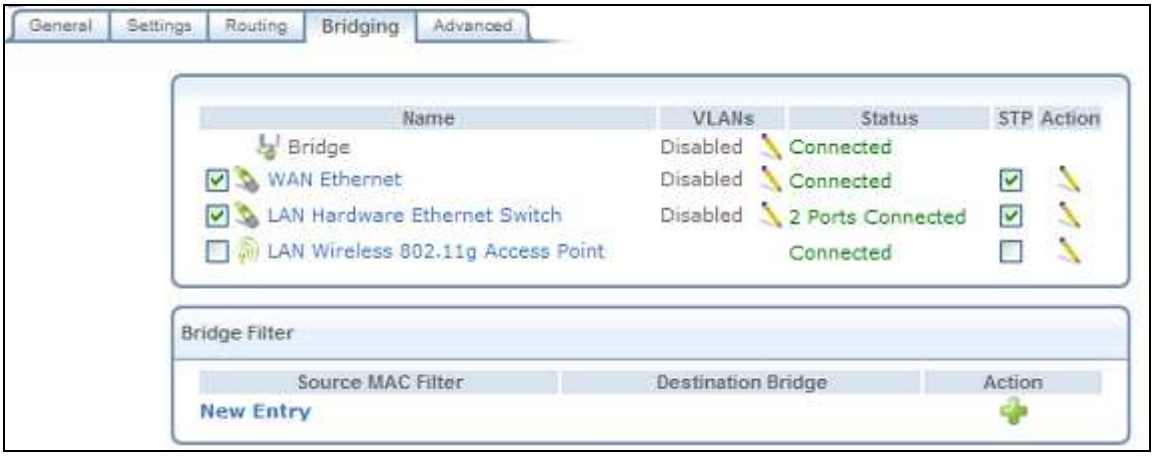
2. Z menu rozwijanego menu „Tryb trasowania" wybierz opcję „Trasa" i kliknij przycisk „Zastosuj". Poniżej na ekranie pojawi się ostrzeżenie.



Rysunek 6.168 Komunikat ostrzegający o potrzebie odświeżenia treści strony

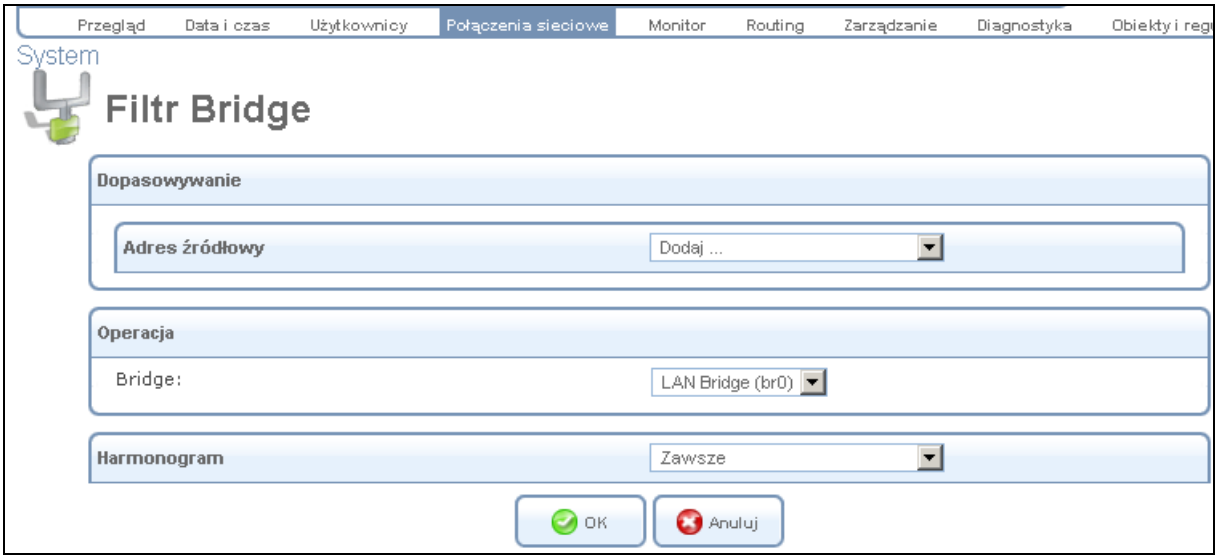
3. Kliknij przycisk „OK". Strona odświeża się podczas zapisywania nowych ustawień i wraca do poprzedniego ekranu.

4. Kliknij zakładkę „Bridging". Wyświetlony zostanie następujący ekran.



Rysunek 6.169 Ustawienia mostu sieciowego WAN-LAN

5. W sekcji „Filtr mostu sieciowego", kliknij link „Nowy wpis". Pojawi się następujący ekran.



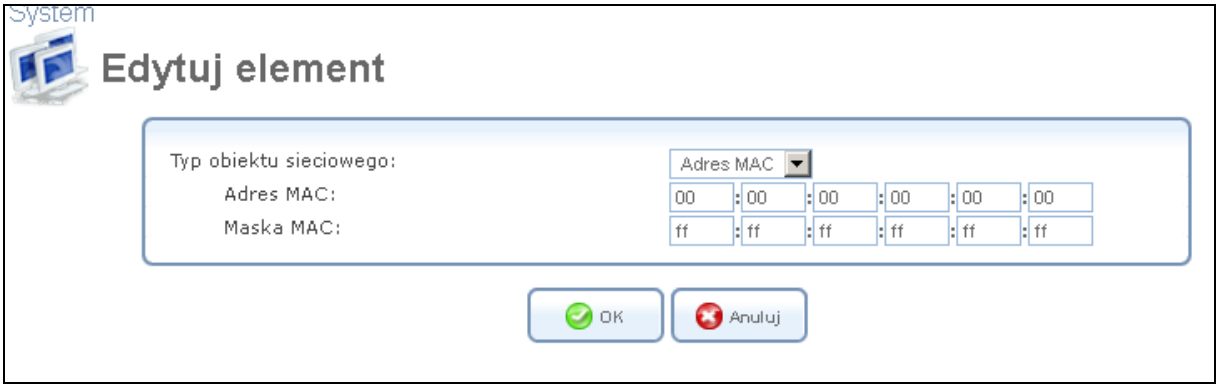
Rysunek 6.170 Ustawienia filtrowania na moście sieciowym

6. Z rozwijanego menu w sekcji „Operacja", zaznacz most WAN-LAN. Jeśli nie widzimy takiej nazwy, jego domyślny wpis pojawia się jako „Bridge (br1)".

7. Z rozwijanego menu „Źródłowy adres" wybierz opcję „Definiowane przez użytkownika".

Rysunek 6.171 Edytuj obiekt sieci

8. Kliknij link „Nowy wpis”.

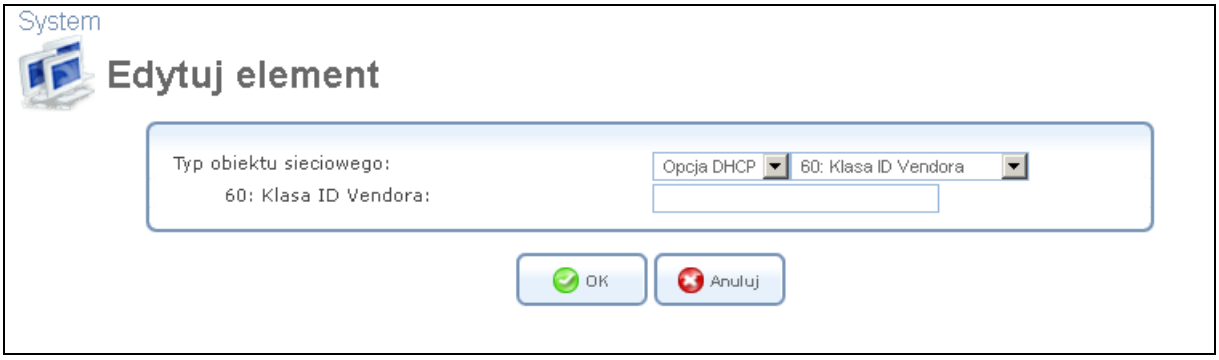


Rysunek 6.172 Edytuj element - Adres MAC

Ten ekran pozwala tworzyć reguły filtrowania ruchu, które umożliwiają bezpośredni przepływ pakietów między interfejsami WAN i LAN, które zostaną dołączone do mostu WAN-LAN. Ta reguła filtrowania może zostać oparta na adresie MAC hosta LAN albo jednej z jego wspomnianych wcześniej opcji DHCP.

9. Jeśli chcesz oprzeć regułę na podstawie adresu MAC, wpisz adres MAC i maskę MAC w odpowiednie pola. W przeciwnym razie wykonaj następujące czynności:

a. Z rozwijanego menu „Typ obiektu sieciowego” wybierz opcję „Opcje DHCP”. Ekran zostanie odświeżony.



Rysunek 6.173 Edycja elementu – opcje DHCP

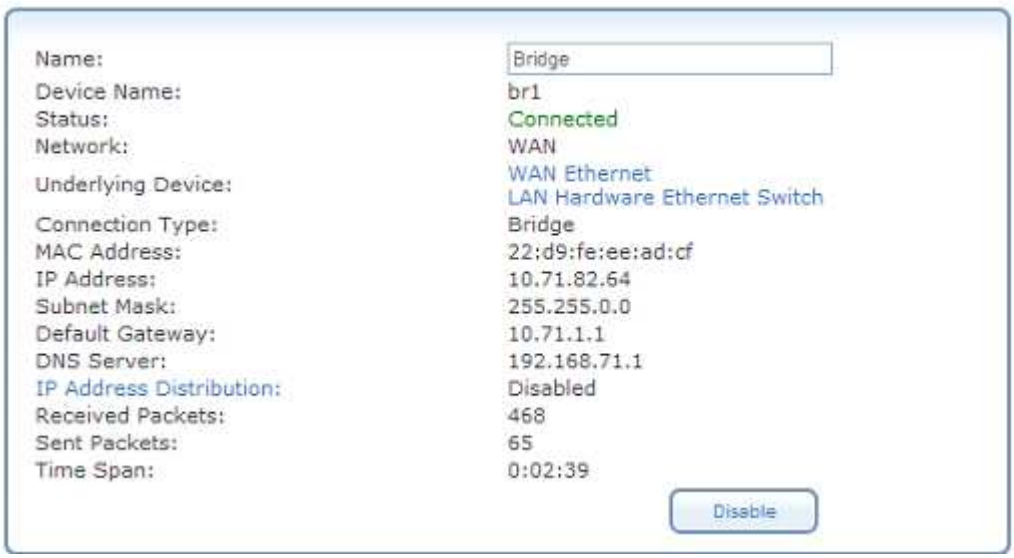
b. Z rozwijanego menu wybierz jedną z opcji DHCP. Pole poniżej odpowiednio zostanie zmienione.

c. Wprowadź odpowiednią wartość dla opcji DHCP (powinny być dostarczone przez usługodawcę lub operatora).

10. Kliknij przycisk „OK", aby zapisać ustawienia.

6.4.13.3 Przeglądania i edytowanie ustawień połączenia

Aby przeglądać i edytować ustawienia połączenia mostu WAN-LAN, kliknij link „Most sieciowy" w sekcji „Połączenia sieciowe". Zostanie wyświetlony ekran z właściwościami połączenia.



Rysunek 6.174 Właściwości mostu sieciowego

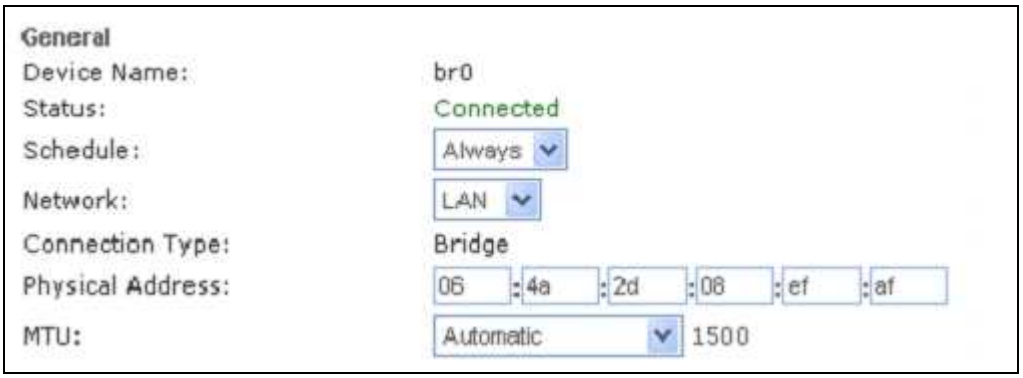
6.4.13.3.1 Ogólne

Ta sekcja umożliwia wyświetlanie ustawień mostu sieciowego WAN-LAN. Wprowadzone ustawienia mogą być edytowane w pozostałej sekcji interfejsu, jak opisano w następujących sekcjach.

6.4.13.3.2 Ustawienia

Sekcja „Ustawienia" pozwala modyfikować następujące ustawienia mostu sieciowego LAN-WAN:

Ogólne - ta sekcja wyświetla ogólne parametry połączenia.



Rysunek 6.175 Ogólne ustawienia mostu sieciowego

Harmonogram - domyślnie połączenie jest zawsze aktywne. Jednakże, można skonfigurować zasady harmonogramu w celu określenia segmentów czasu, w którym połączenie może być aktywne. Po wybraniu zdefiniowanej reguły, z rozwijanego menu pozwala na wybór pomiędzy dostępnymi regułami. Aby dowiedzieć się jak skonfigurować reguły harmonogramu, możemy odnieść się do „Definiowania reguł harmonogramu" w części administracyjnej instrukcji OpenRG.

Sieć - wybierz, czy parametry konfigurowane odnoszą się do połączenia WAN, LAN lub DMZ wybierając typ połączenia z rozwijanego menu. Aby uzyskać więcej informacji, odnoszących się do powyższej funkcji, możemy ich znaleźć w sekcji „Typy sieci"

administracyjnej instrukcji OpenRG. Należy pamiętać, że przy definiowaniu połączenia sieci jako DMZ, należy także:

• Odłączyć połączenie z mostu, jeśli takie istnieje.
• Zmiana trybu połączenia trasy do „Router", w „Routingu".
• Dodaj reguły routingu na zewnątrz bramy (które mogą być dostarczane przez ISP), informuj sieć DMZ za OpenRG.

Adres fizyczny – pole adresu fizycznego MAC interfejsu sieciowego. Niektóre interfejsy pozwalają na zmianę wartości adresu MAC.

Klonuj mój adres MAC - naciśnij ten przycisk, aby skopiować aktualny adres MAC z karty sieciowej komputera.

MTU - MTU jest to maksymalna jednostka transmisji. Określa ona największy rozmiar pakietu, jakim możemy przekazywać dane do Internetu. W ustawieniach domyślnych, automatycznie brama wybiera najlepsze MTU dla połączenia internetowego. Wybierz opcję „Automatycznie przez serwer DHCP", wtedy DHCP określenia wielkość MTU. W przypadku wybrania opcji „Ręcznie" zaleca się wpisać wartość od 1200 do 1500.

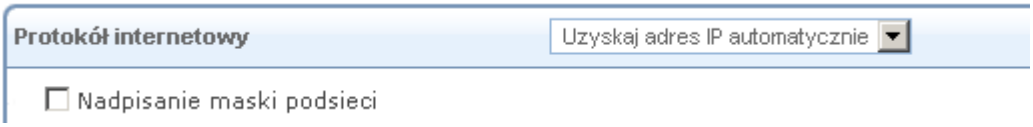
Protokół internetowy - wybierz jedną z następujących opcji protokołu internetowego
• Nienumerowany
• Uzyskaj adres IP automatycznie
• Użyj następującego adresu IP

Zwróć uwagę, że ekran zostanie odświeżony, aby wyświetlić odpowiednie ustawienia zgodnie z Twoim wyborem.

Brak adresu IP - wybierz „Brak adresu IP", jeśli wymaga się, żeby brama nie posiadała adresu IP. Opcja ta może być użyteczna, jeśli pracujesz w środowisku, w które nie jest podłączone do innych sieci, takich jak Internet.

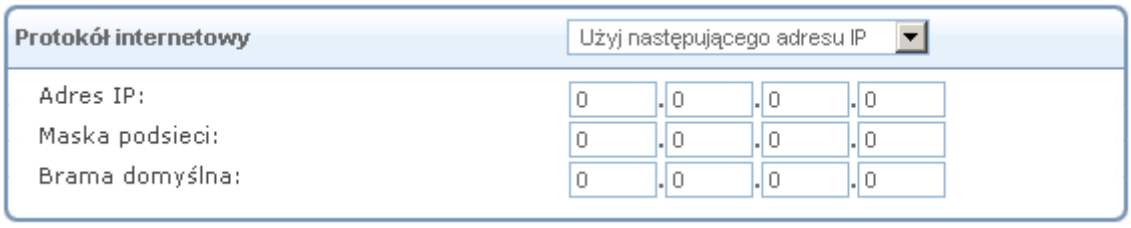
Rysunek 6.176 Protokół internetowy - Brak adresu IP

Uzyskaj adres IP automatycznie - połączenie jest domyślnie skonfigurowane do pracy jako klient DHCP. Należy zachować tą konfigurację w przypadku, gdy usługodawca obsługuje DHCP lub jeśli łączysz się za pomocą dynamicznego adresu IP. Serwer operatora, przypisuje parametry bramy adresem IP i wyznacza maskę podsieci. Możesz zmienić dynamiczną maskę podsieci przypisaną przez DHCP, wybierając opcję „Zastąp maskę podsieci" i określ własną maskę zamiast przypisanej. Można kliknąć przycisk „Zwolnij", aby zwolnić bieżącą dzierżawę adresu IP. Po kliknięciu „Zwolnij" adres został zwolniony, należy kliknąć „Odnów". Użyj przycisku „Odnów" odnowienia dzierżawę adresu IP.



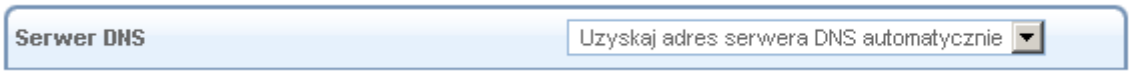
Rysunek 6.177 Automatyczne uzyskiwanie parametrów interfejsu

Użyj następującego adresu IP - połączenie można skonfigurować za pomocą stałego (statycznego) adresu IP. Usługodawca powinien zapewnić wtedy taki adresu IP i maskę podsieci.



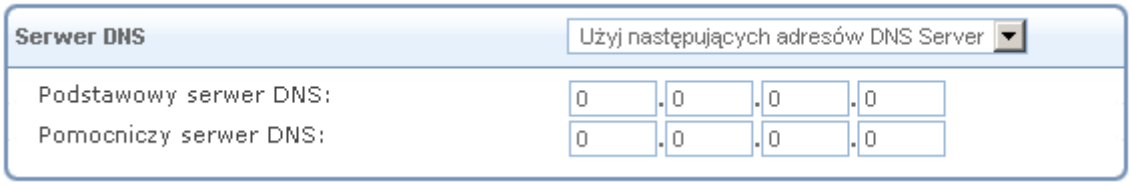
Rysunek 6.178 Protokół internetowy – Statyczne IP

Serwer DNS - Domain Name System (DNS) jest metodą, w której nazwy domeny witryny sieci www są tłumaczone na adresy IP. Możesz skonfigurować połączenie do automatycznego uzyskania adresów serwera DNS, albo określić takiego adresy ręcznie, zgodnie z informacjami dostarczanymi przez ISP. Aby skonfigurować połączenie do automatycznego uzyskania serwera DNS, wybierz opcję „Uzyskaj adres serwera DNS automatycznie" z rozwijanego menu „Serwer DNS".



Rysunek 6.179 Serwer DNS – Automatyczne uzyskiwanie parametrów

Aby ręcznie skonfigurować adresy serwerów DNS, wybierz opcję „Użyj następujących serwerów DNS" z rozwijanego menu (patrz rysunek „Serwer DNS - Statyczne IP"). Określ do dwóch różnych adresów serwera DNS, pierwotny i zapasowy.

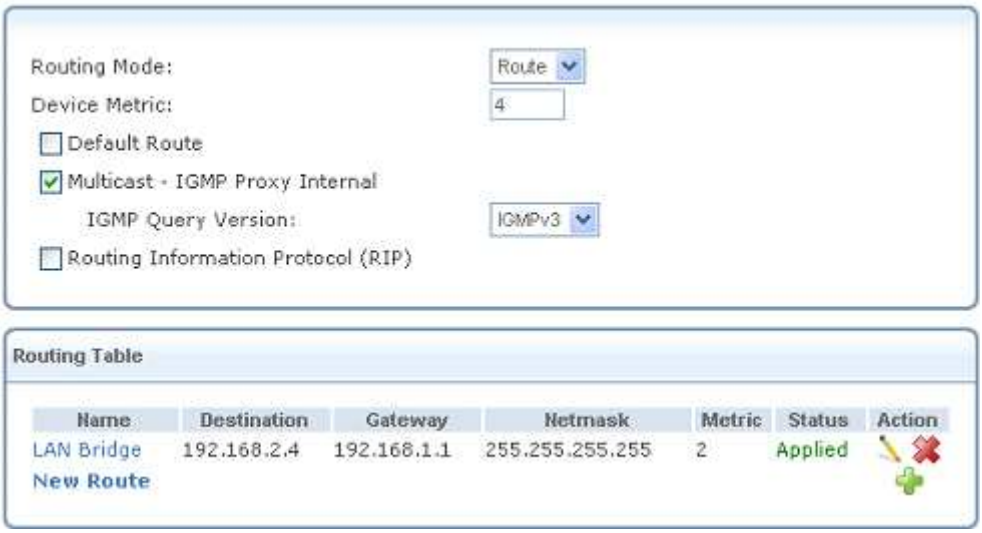


Rysunek 6.180 Serwer DNS - Statyczne IP

Dystrybucja adresów IP - ogólnie rzecz biorąc, sekcja dystrybucji adresów IP pozwala na konfigurowanie parametrów serwera DHCP. Jednakże w konfiguracji mostu sieciowego WAN-LAN, serwer DHCP musi być wyłączony.

6.4.13.3.3 Routing

Ta zakładka umożliwia skonfigurowanie ustawień trasowania połączenia. Można wybrać i skonfigurować bramę do statycznego lub dynamicznego routingu. Routing dynamiczny automatycznie dostosowuje tablice trasowania do ruchu pakietów w sieci. Routing statyczny określa stałą ścieżkę do innych podsieci.



Rysunek 6.181 Zaawansowane właściwości trasowania

Możesz skonfigurować następujące ustawienia:

Tryb trasowania - wybierz jeden z następujących trybów trasy:

Trasa - użyj tej funkcji, jeśli chcesz , aby brama działania jako router między dwoma sieciami.

NAPT - Network Address Port Translation (NAPT) odnosi się do procesu translacji adresów z udziałem mapowania numerów portów, dzięki czemu wiele maszyn przy posiadaniu jednego publicznego adresu IP. Użyj NAPT, jeśli LAN obejmuje wiele urządzeń, topologii, które wymagają tłumaczenia port oprócz translacji adresów.

Device metric (metryka urządzenia) - jest wartością używaną przez bramę w celu określenia, czy jedna trasa jest lepsza od innej, biorąc pod uwagę takie parametry jak przepustowość, opóźnienie i wiele innych.

Trasa domyślna - zaznacz to pole wyboru w celu określenia tego urządzenia jako domyślnej trasy.

Multicast - domyślne proxy IGMP - OpenRG służy jako serwer proxy IGMP, wydawanie przyjmowanych komunikatów IGMP w imieniu podłączonych komputerów z sieci lokalnej. To pole wyboru jest aktywne domyślnie w sieci LAN, co oznacza, że jeśli serwer multicast jest dostępny w LAN, inne komputery z sieci LAN wyślą prośbę, aby dołączyć do grup multicast (wyślą żądanie IGMP). Jednak to pole wyboru jest wyłączone domyślnie dla połączenia WAN, co oznacza, że komputery z sieci lokalnej nie będą w stanie dołączyć do grupy multicast WAN serwerów multicast. Podczas tworzenia mostu sieciowego WAN-LAN, to pole wyboru musi być odznaczone.

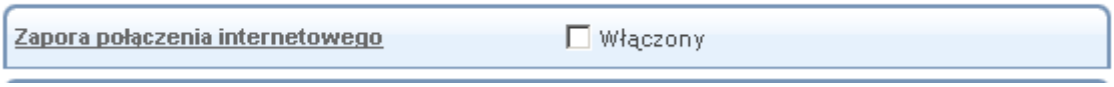
Wersja IGMP Query - OpenRG obsługuje wszystkie trzy wersje IGMP. Wybierz wersję, której chcesz użyć. Pamiętaj, że menu rozwijane pojawia się tylko podczas połączenia LAN.

Tabela routingu - umożliwia dodanie lub zmianę trasy, gdy urządzenie jest aktywne. Użyj przycisku „Nowa trasa", aby dodać trasy lub edytować istniejące trasy.

6.4.13.3.4 Zaawansowane

Ta sekcja pozwala skonfigurować ustawienia zaawansowane połączenia.

• **Zapora połączenia internetowego** - Twoja zapora sieciowa urządzenia pomaga chronić komputer poprzez zapobieganie nieautoryzowanym uzyskaniem dostępu przez użytkowników za pośrednictwem sieci, takiej jak Internet. Zapora sieciowa może być aktywowana na danym połączeniu sieciowym. Aby włączyć zapory dla połączenia sieciowego, zaznacz pole wyboru „Włączony". Aby dowiedzieć się jak najwięcej na temat zabezpieczeń bramy, patrz punkt 5.2.



Rysunek 6.182 Zapora połączenia internetowego

• **Dodatkowe adresy IP** - można dodać aliasy (dodatkowe adresy IP) bramy, klikając na link „Nowy adres IP". Pozwala to dostępu do bramy za pomocą aliasów oprócz domyślnego 192.168.1.254 i http://netiaspot.home.

Rysunek 6.183 Dodatkowe adresy IP

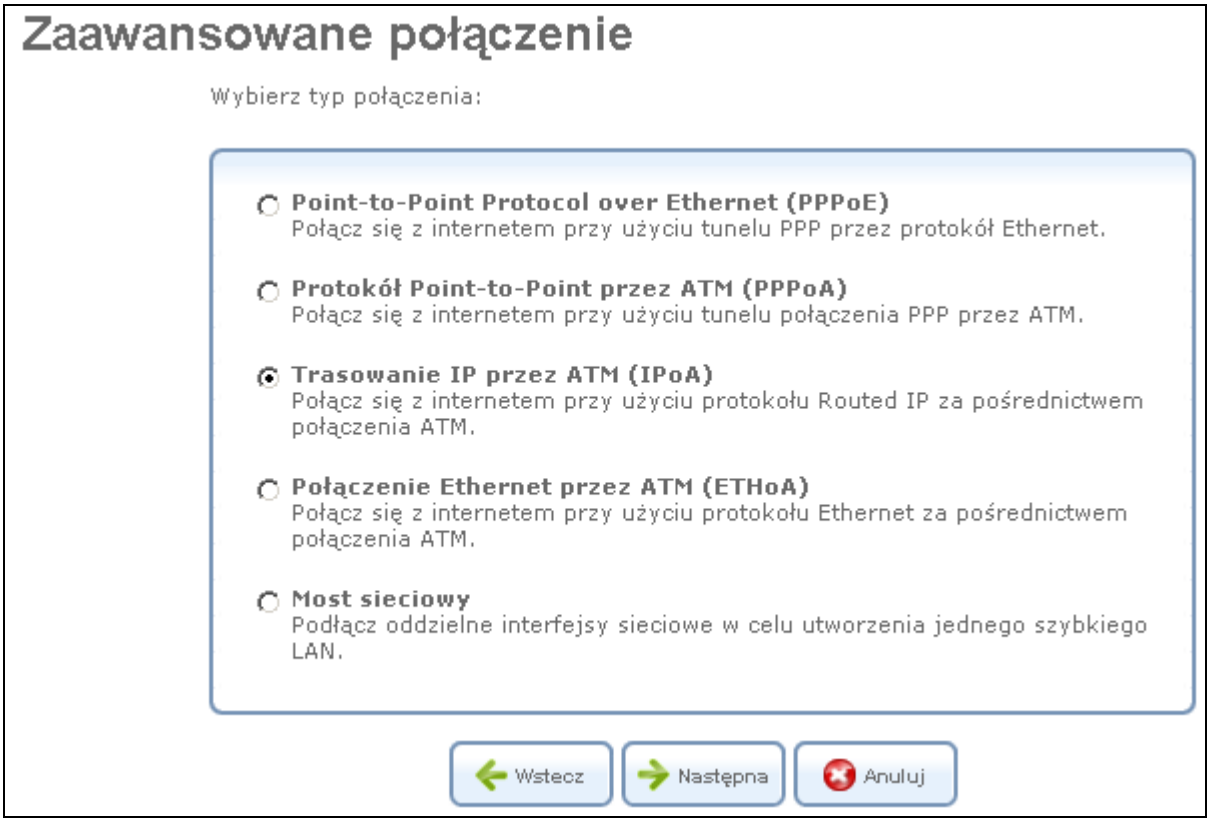
6.4.14 Konfigurowanie połączenia Routed IP przez ATM

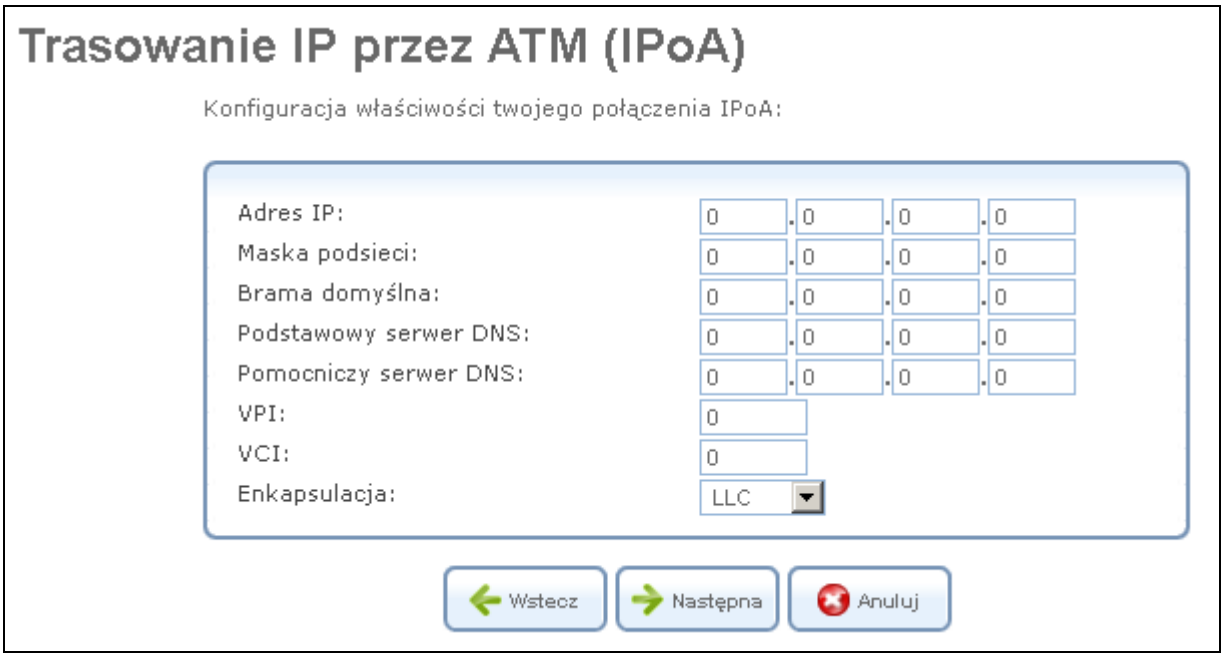
Trasowanie IP przez ATM (IPoA) jest standardem przekazywania ruchu IP w sieci ATM.

6.4.14.1 Tworzenia połączenia IPoA

Aby utworzyć nowe połączenie IPoA, wykonaj następujące czynności:

1. Kliknij przycisk „Nowe połączenie" link w sekcji „Połączenia sieciowe" (patrz rysunek 6.10). Wyświetlony zostanie ekran kreatora połączeń (patrz rysunek 6.18).
2. Wybierz „Połączenie zaawansowane", a następnie przycisk „Dalej". Wyświetlony zostanie ekran „Połączenie zaawansowane" (patrz rysunek 6.20).
3. Zaznacz „Trasowanie IP przez ATM (IPoA)", a następnie przycisk „Dalej".





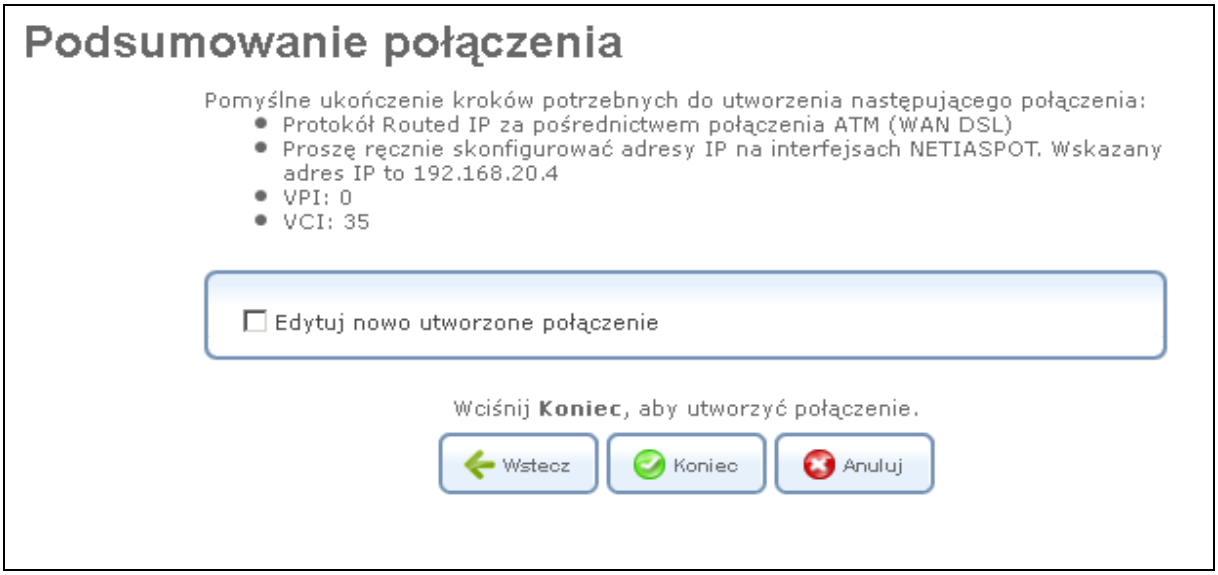
Rysunek 6.184 Trasowanie IP przez ATM

4. Wprowadź następujące informacje, które powinny być dostarczane przez usługodawcę:

- Adres IP

- Maska podsieci
- Brama domyślna
- Podstawowy serwer DNS
- Pomocniczy serwer DNS
- Identyfikator pary VPI/VCI
- Sposób enkapsulacji: LLC lub VCMux

5. Kliknij przycisk „Dalej”. Wyświetlony zostanie ekran „Podsumowanie połączenia”.



Rysunek 6.185 Podsumowanie połączenia

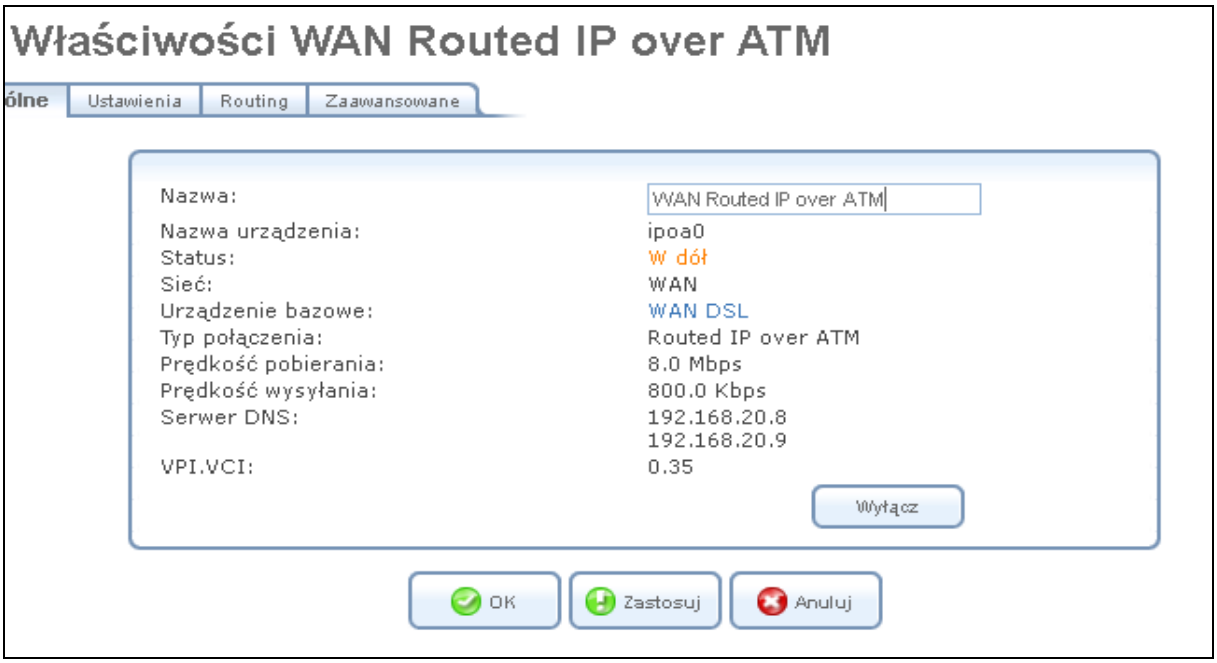
6. Wybierz pole wyboru „Edytuj nowo utworzone połączenie”, jeśli chcesz być skierowany do nowego ekranu konfiguracji połączenia po kliknięciu przycisku „Koniec”. Ekran ten jest opisany w dalszej części tego rozdziału.

7. Kliknij przycisk „Koniec”, aby zapisać ustawienia. Nowy połączenie zostanie dodane do listy połączeń sieci i będzie konfigurowane, jak każde inne połączenie.

Nowe połączenie IPoA zostanie dodane do listy połączeń sieciowych i będziemy mogli go konfigurować, jak każde inne połączenie.

6.4.14.2 Przeglądanie i edytowanie ustawień połączenia

Aby wyświetlić i zmienić ustawienia połączenia IPoA, kliknij na link „WAN IPoA" w sekcji „Połączenia sieciowe", wyświetlone zostaną właściwości połączenia „Trasowanie IP przez ATM".



Rysunek 6.186 Właściwości połączenia

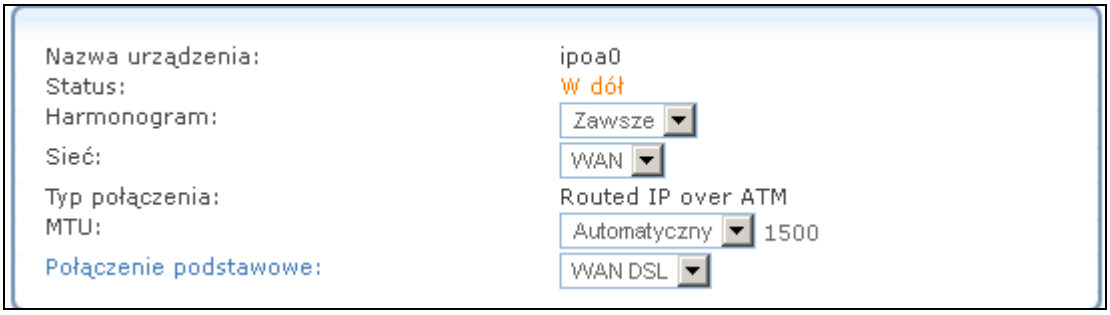
6.4.14.2.1 Ogólne

Ta sekcja umożliwia wyświetlanie ustawień połączenia IPoA (patrz rys. 6.186). Wprowadzone ustawienia mogą być edytowane w pozostałej sekcji interfejsu, jak opisano w następujących sekcjach.

6.4.14.2.2 Ustawienia

Sekcja „Ustawienia" pozwala modyfikować następujące ustawienia IPoA:

Ogólne - ta sekcja wyświetla ogólne parametry połączenia.



Rysunek 6.187 Ogólne ustawienia IPoA

Harmonogram - domyślnie połączenie jest zawsze aktywne. Jednakże, można skonfigurować zasady harmonogramu w celu określenia segmentów czasu, w którym połączenie może być aktywne. Po wybraniu zdefiniowanej reguły, z rozwijanego menu pozwala na wybór pomiędzy dostępnymi regułami. Aby dowiedzieć się, jak skonfigurować reguły harmonogramu, możemy odnieść się do „Definiowania reguł harmonogramu" w części administracyjnej instrukcji OpenRG.

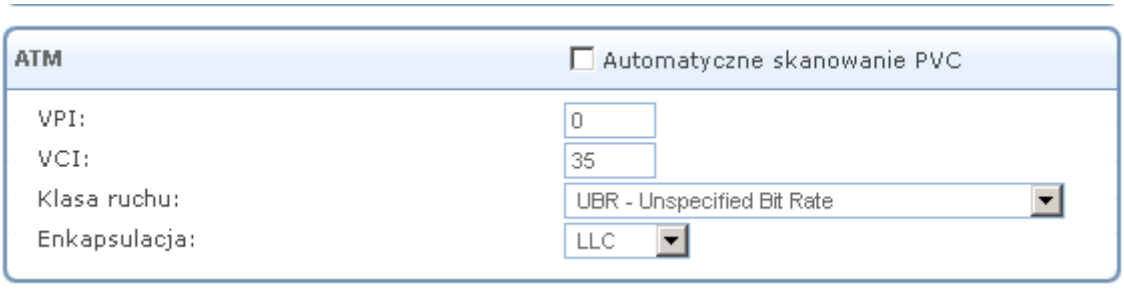
Sieć - wybierz, czy parametry konfigurowane odnoszą się do połączenia WAN, LAN lub DMZ wybierając typ połączenia z rozwijanego menu. Aby uzyskać więcej informacji, odnoszących się do powyższej funkcji, możemy ich znaleźć w sekcji „Typy sieci" administracyjnej instrukcji OpenRG. Należy pamiętać, że przy definiowaniu połączenia sieci jako DMZ, należy także:

• Odłączyć połączenie z mostu, jeśli takie istnieje.
• Zmiana trybu połączenia trasy do „Router", w „Routingu".
• Dodaj reguły routingu na zewnątrz bramy (które mogą być dostarczane przez ISP), informuj sieć DMZ za OpenRG.

MTU - MTU jest to maksymalna jednostka transmisji. Określa ona największy rozmiar pakietu, jakim możemy przekazywać dane do Internetu. W ustawieniach domyślnych, automatycznie brama wybiera najlepsze MTU dla połączenia internetowego. Wybierz opcję „Automatycznie przez serwer DHCP", wtedy DHCP określenia wielkość MTU. W przypadku wybrania opcji „Ręcznie" zaleca się wpisać wartość od 1200 do 1500.

Połączenie bazowe - określa podstawowe połączenia, powyżej którego protokół będzie zainicjowany.

ATM - Asynchronous Transfer Mode (ATM) to technologia oparta na przesyłania danych w sieciach komórkowych lub pakietów o stałej wielkości. Używane komórki ATM są stosunkowo niewielkie w porównaniu do jednostek używanych w innych technologiach. Mała, stała wielkość komórek pozwala na transmisję wideo, audio i danych komputerowych, zapewniając, że żaden pojedynczy typ danych nie zużyje połączenia. Adresowanie ATM składa się z dwóch identyfikatorów, które określają ścieżkę wirtualną (VPI) i wirtualne połączenie (VCI). Ścieżka wirtualna składa się z wielu kanałów wirtualnych do tego samego punktu końcowego. Enkapsulacja do połączenia powinna być ustawiona jako „LLC" lub „VCMux". Należy skonfigurować te parametry zgodnie z informacjami przekazanymi przez ISP.



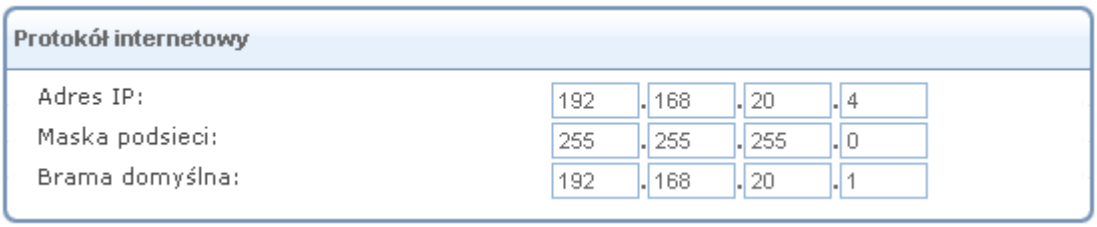
Rysunek 6.188 Ustawienia ATM

Protokół internetowy - wybierz jedną z następujących opcji protokołu internetowego

• Nienumerowany

• Uzyskaj adres IP automatycznie

• Użyj następującego adresu IP

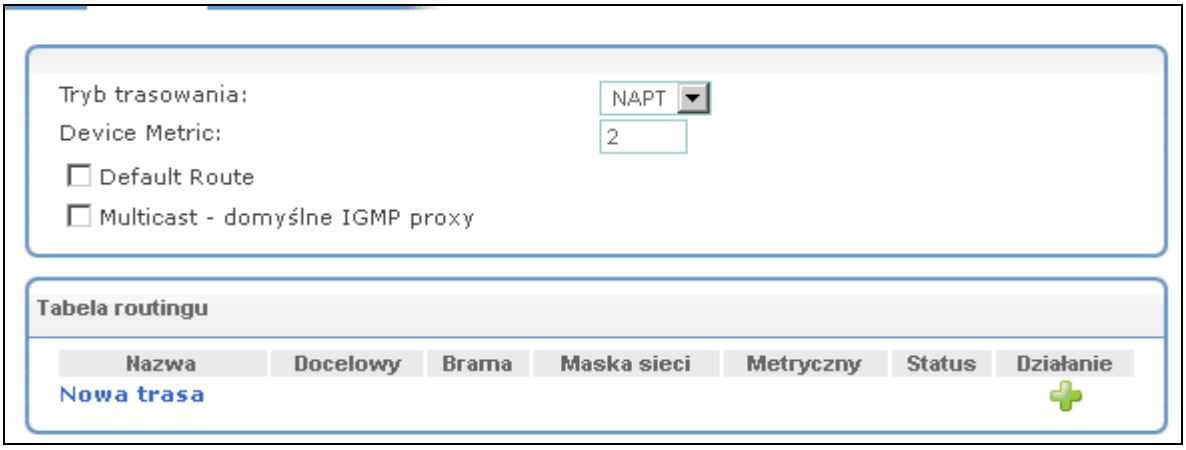


Rysunek 6.189 Protokół internetowy

Zwróć uwagę, że ekran zostanie odświeżony, aby wyświetlić odpowiednie ustawienia zgodnie z Twoim wyborem.

6.4.14.2.3 Trasowanie

Ta zakładka umożliwia skonfigurowanie ustawień trasowania połączenia. Można wybrać i skonfigurować bramę do statycznego lub dynamicznego routingu. Routing dynamiczny automatycznie dostosowuje tablice trasowania do ruchu pakietów w sieci. Routing statyczny określa stałą ścieżkę do innych podsieci.



Rysunek 6.190 Zaawansowane właściwości trasowania

Możesz skonfigurować następujące ustawienia:

Tryb trasowania - wybierz jeden z następujących trybów trasy:

Trasa - użyj tej funkcji, jeśli chcesz , aby brama działania jako router między dwoma sieciami.

NAPT - Network Address Port Translation (NAPT) odnosi się do procesu translacji adresów z udziałem mapowania numerów portów, dzięki czemu wiele maszyn przy posiadaniu jednego publicznego adresu IP. Użyj NAPT, jeśli LAN obejmuje wiele urządzeń, topologii, które wymagają tłumaczenia port oprócz translacji adresów.

Device metric (metryka urządzenia) - jest wartością używaną przez bramę w celu określenia, czy jedna trasa jest lepsza od innej, biorąc pod uwagę takie parametry jak przepustowość, opóźnienie i wiele innych.

Trasa domyślna - zaznacz to pole wyboru w celu określenia tego urządzenia jako domyślnej trasy.

Multicast - domyślne proxy IGMP - OpenRG służy jako serwer proxy IGMP, wydawanie przyjmowanych komunikatów IGMP w imieniu podłączonych komputerów z sieci lokalnej. To pole wyboru jest aktywne domyślnie w sieci LAN, co oznacza, że jeśli serwer multicast jest dostępny w LAN, inne komputery z sieci LAN wyślą prośbę, aby dołączyć do grup multicast (wyślą żądanie IGMP). Jednak to pole wyboru jest wyłączone domyślnie dla połączenia WAN, co oznacza, że komputery z sieci lokalnej nie będą w stanie dołączyć do grupy multicast WAN serwerów multicast. Podczas tworzenia mostu sieciowego WAN-LAN, to pole wyboru musi być odznaczone.

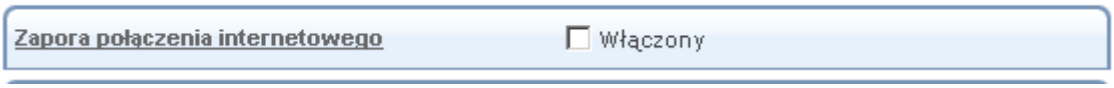
Wersja IGMP Query - OpenRG obsługuje wszystkie trzy wersje IGMP. Wybierz wersję, której chcesz użyć. Pamiętaj, że menu rozwijane pojawia się tylko podczas połączenia LAN.

Tabela routingu - umożliwia dodanie lub zmianę trasy, gdy urządzenie jest aktywne. Użyj przycisku „Nowa trasa", aby dodać trasy lub edytować istniejące trasy.

6.4.14.2.4 Zaawansowane

Ta sekcja pozwala skonfigurować ustawienia zaawansowane interfejsu IPoA.

• **Zapora połączenia internetowego** - Twoja zapora sieciowa urządzenia pomaga chronić komputer poprzez zapobieganie nieautoryzowanym uzyskaniem dostępu przez użytkowników za pośrednictwem sieci, takiej jak Internet. Zapora sieciowa może być aktywowana na danym połączeniu sieciowym. Aby włączyć zapory dla połączenia sieciowego, zaznacz pole wyboru „Włączony". Aby dowiedzieć się jak najwięcej na temat zabezpieczeń bramy, patrz punkt 5.2.



Rysunek 6.191 Zapora połączenia internetowego

6.4.15 Serial PPP

Serial PPP jest logicznym połączeniem sieci WAN 3G przez zewnętrzny modem USB.

6.4.15.1 Przeglądanie i edytowanie ustawień połączenia

Aby wyświetlić i zmienić ustawienia połączenia PPP, kliknij na link „Serial PPP" w ekranie „Połączenia sieciowe". Wyświetlone zostanie ekran „Właściwości Serial PPP".

Rysunek 6.192 Właściwości połączenia 3G

6.4.15.1.1 Ogólne

Ta sekcja umożliwia wyświetlanie ustawień połączenia Serial PPP. Wprowadzone ustawienia mogą być edytowane w pozostałej sekcji interfejsu, jak opisano w następujących sekcjach. Dodatkowo możemy włączyć lub wyłączyć interfejs 3G.

6.4.15.1.2 Ustawienia

Sekcja „Ustawienia" pozwala modyfikować następujące ustawienia połączenia Serial PPP:

Ogólne - ta sekcja wyświetla ogólne parametry połączenia.

Rysunek 6.193 Ogólne ustawienia połączenia Serial PPP

Harmonogram - domyślnie połączenie jest zawsze aktywne. Jednakże, można skonfigurować zasady harmonogramu w celu określenia segmentów czasu, w którym połączenie może być aktywne. Po wybraniu zdefiniowanej reguły, z rozwijanego menu pozwala na wybór pomiędzy dostępnymi regułami. Aby dowiedzieć się, jak skonfigurować reguły harmonogramu, możemy odnieść się do „Definiowania reguł harmonogramu" w części administracyjnej instrukcji OpenRG.

Sieć - wybierz, czy parametry konfigurowane odnoszą się do połączenia WAN, LAN lub DMZ wybierając typ połączenia z rozwijanego menu. Aby uzyskać więcej informacji, odnoszących się do powyższej funkcji, możemy ich znaleźć w sekcji „Typy sieci" administracyjnej instrukcji OpenRG. Należy pamiętać, że przy definiowaniu połączenia sieci jako DMZ, należy także:

• Odłączyć połączenie z mostu, jeśli takie istnieje.
• Zmiana trybu połączenia trasy do „Router", w „Routingu".
• Dodaj reguły routingu na zewnątrz bramy (które mogą być dostarczane przez ISP), informuj sieć DMZ za OpenRG.

MTU - MTU jest to maksymalna jednostka transmisji. Określa ona największy rozmiar pakietu, jakim możemy przekazywać dane do Internetu. W ustawieniach domyślnych, automatycznie brama wybiera najlepsze MTU dla połączenia internetowego. Wybierz opcję „Automatycznie przez serwer DHCP", wtedy DHCP określenia wielkość MTU. W przypadku wybrania opcji „Ręcznie" zaleca się wpisać wartość od 1200 do 1500.

Połączenie bazowe - określa podstawowe połączenia, powyżej którego protokół będzie zainicjowany.

Protokół internetowy - wybierz jedną z następujących opcji protokołu internetowego

• Nienumerowany
• Uzyskaj adres IP automatycznie
• Użyj następującego adresu IP

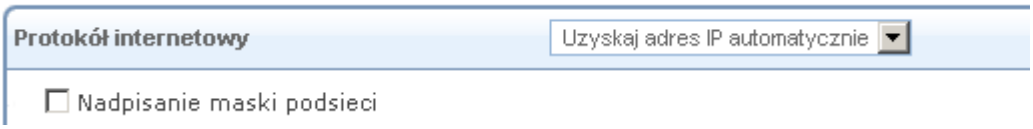
Zwróć uwagę, że ekran zostanie odświeżony, aby wyświetlić odpowiednie ustawienia zgodnie z Twoim wyborem.

Nienumerowany - wybierz tę opcję, aby przypisać wstępnie adres LAN jako adres WAN OpenRG. Jest to przydatne podczas, gdy OpenRG pracuje w trybie routingu. Przed wybraniem tej opcji należy, skonfigurować sekcję „Protokół internetowy" urządzenia sieci LAN (lub most sieciowy w przypadku, gdy urządzenie LAN jest mostem sieciowym) użyć statycznego adresu IP z zakresu adresów IP dostarczonych przez usługodawcę internetowego (zamiast 192.168.1.254).

Rysunek 6.194 Protokół internetowy – nienumerowany

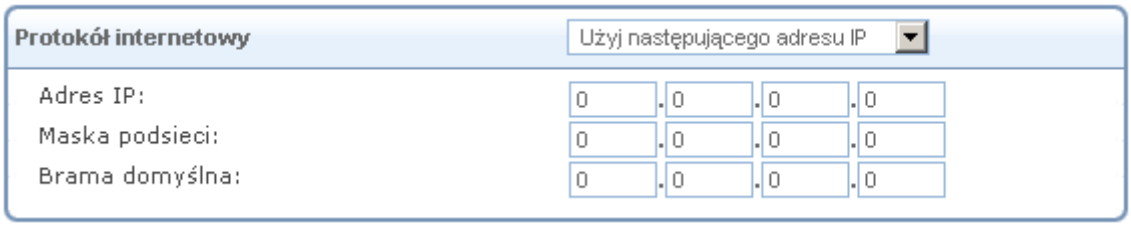
Uzyskaj adres IP automatycznie - połączenie jest domyślnie skonfigurowane do pracy jako klient DHCP. Należy zachować tą konfigurację w przypadku, gdy usługodawca obsługuje DHCP lub jeśli łączysz się za pomocą dynamicznego adresu IP. Serwer operatora, przypisuje parametry bramy adresem IP i wyznacza maskę podsieci. Możesz zmienić

dynamiczną maskę podsieci przypisaną przez DHCP, wybierając opcję „Zastąp maskę podsieci" i określ własną maskę zamiast przypisanej. Można kliknąć przycisk „Zwolnij", aby zwolnić bieżącą dzierżawę adresu IP. Po kliknięciu „Zwolnij" adres został zwolniony, należy kliknąć „Odnów". Użyj przycisku „Odnów" odnowienia dzierżawę adresu IP.



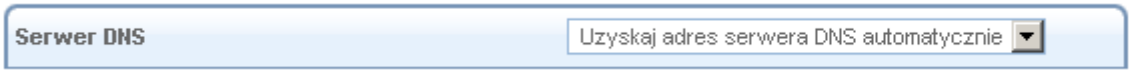
Rysunek 6.195 Automatyczne uzyskiwanie parametrów interfejsu

Użyj następującego adresu IP - połączenie można skonfigurować za pomocą stałego (statycznego) adresu IP. Usługodawca powinien zapewnić wtedy taki adresu IP i maskę podsieci.



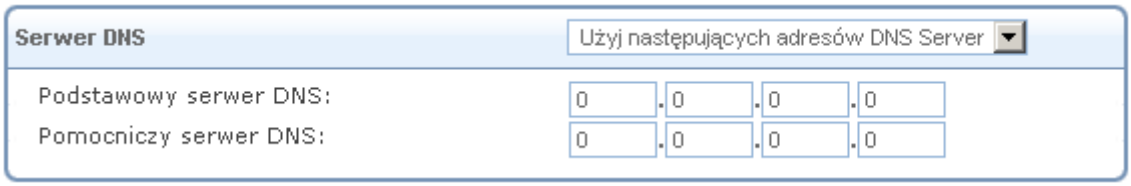
Rysunek 6.196 Protokół internetowy – Statyczne IP

Serwer DNS - Domain Name System (DNS) jest metodą, w której nazwy domeny witryny sieci www, są tłumaczone na adresy IP. Możesz skonfigurować połączenie do automatycznego uzyskania adresów serwera DNS, albo określić takiego adresy ręcznie, zgodnie z informacjami dostarczanymi przez ISP. Aby skonfigurować połączenie do automatycznego uzyskania serwera DNS, wybierz opcję „Uzyskaj adres serwera DNS automatycznie" z rozwijanego menu „Serwer DNS".



Rysunek 6.197 Serwer DNS – Automatyczne uzyskiwanie parametrów

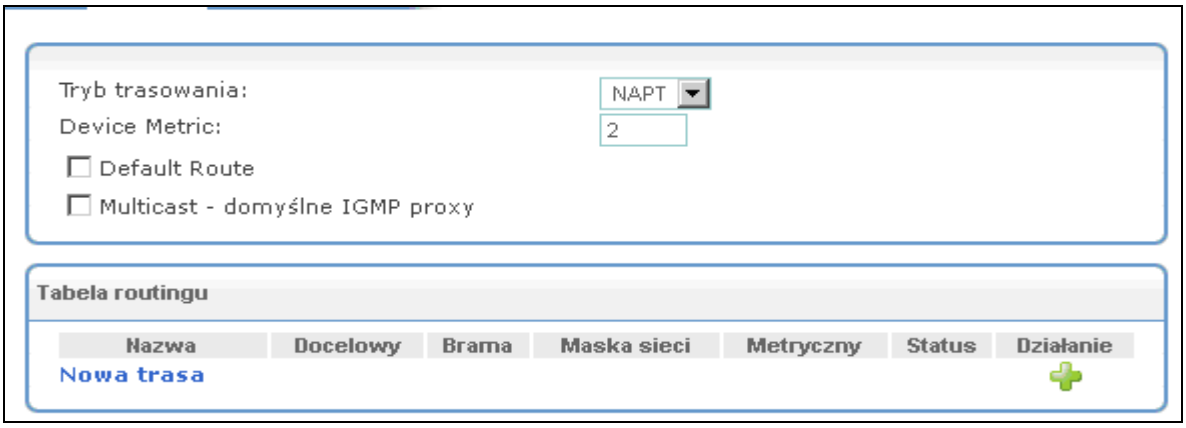
Aby ręcznie skonfigurować adresy serwerów DNS, wybierz opcję „Użyj następujących serwerów DNS" z rozwijanego menu (patrz rysunek „Serwer DNS - Statyczne IP"). Określ do dwóch różnych adresów serwera DNS, pierwotny i zapasowy.



Rysunek 6.198 Serwer DNS - Statyczne IP

6.4.15.1.3 Routing

Ta zakładka umożliwia skonfigurowanie ustawień trasowania połączenia. Można wybrać i skonfigurować bramę do statycznego lub dynamicznego routingu. Routing dynamiczny automatycznie dostosowuje tablice trasowania do ruchu pakietów w sieci. Routing statyczny określa stałą ścieżkę do innych podsieci.



Rysunek 6.199 Zaawansowane właściwości trasowania

Możesz skonfigurować następujące ustawienia:

Tryb trasowania - wybierz jeden z następujących trybów trasy:

Trasa - użyj tej funkcji, jeśli chcesz , aby brama działania jako router między dwoma sieciami.

NAPT - Network Address Port Translation (NAPT) odnosi się do procesu translacji adresów z udziałem mapowania numerów portów, dzięki czemu wiele maszyn przy posiadaniu

jednego publicznego adresu IP. Użyj NAPT, jeśli LAN obejmuje wiele urządzeń, topologii, które wymagają tłumaczenia port oprócz translacji adresów.

Device metric (metryka urządzenia)- jest wartością używaną przez bramę w celu określenia, czy jedna trasa jest lepsza od innej, biorąc pod uwagę takie parametry jak przepustowość, opóźnienie i wiele innych.
Trasa domyślna - zaznacz to pole wyboru w celu określenia tego urządzenia jako domyślnej trasy.

Multicast - domyślne proxy IGMP - OpenRG służy jako serwer proxy IGMP, wydawanie przyjmowanych komunikatów IGMP w imieniu podłączonych komputerów z sieci lokalnej. To pole wyboru jest aktywne domyślnie w sieci LAN, co oznacza, że jeśli serwer multicast jest dostępny w LAN, inne komputery z sieci LAN wyślą prośbę, aby dołączyć do grup multicast (wyślą żądanie IGMP). Jednak to pole wyboru jest wyłączone domyślnie dla połączenia WAN, co oznacza, że komputery z sieci lokalnej nie będą w stanie dołączyć do grupy multicast WAN serwerów multicast. Podczas tworzenia mostu sieciowego WAN-LAN, to pole wyboru musi być odznaczone.

Wersja IGMP Query - OpenRG obsługuje wszystkie trzy wersje IGMP. Wybierz wersję, której chcesz użyć. Pamiętaj, że menu rozwijane pojawia się tylko podczas połączenia LAN.

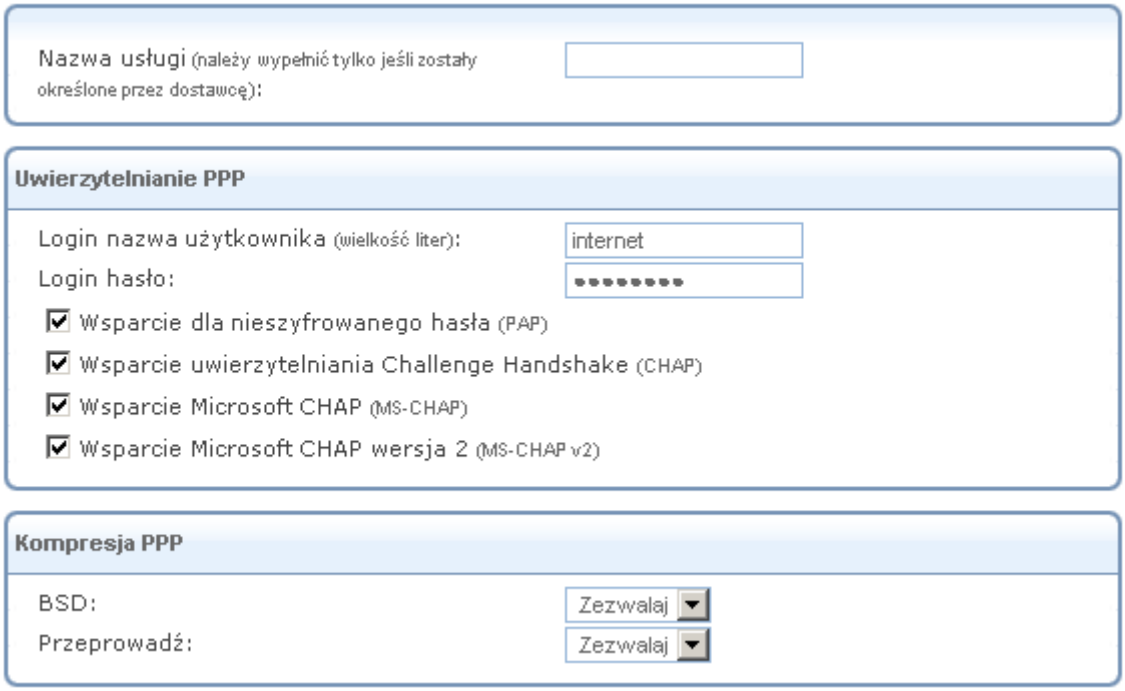
Tabela routingu - umożliwia dodanie lub zmianę trasy, gdy urządzenie jest aktywne. Użyj przycisku „Nowa trasa", aby dodać trasy lub edytować istniejące trasy.

6.4.15.1.4 PPP

Point-to-Point Protocol (PPP) jest najbardziej popularną metodą transportu pakietów pomiędzy użytkownikiem a dostawcą usług internetowych. PPP obsługuje protokoły uwierzytelniania, takie jak PAP i CHAP, jak również inne takie jak kompresje i protokoły szyfrowania.

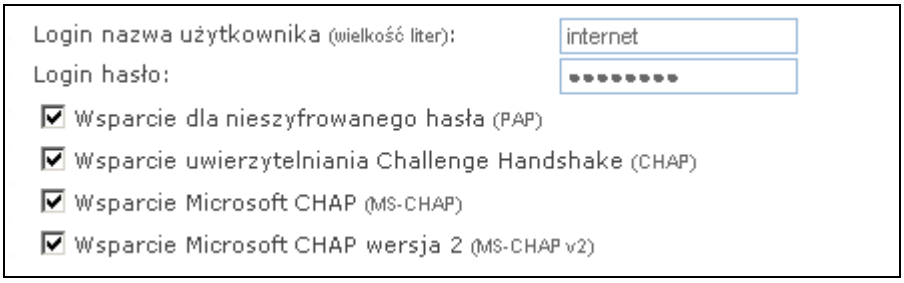
PPP na żądanie – opcja PPP na żądanie rozpoczyna sesję punkt-punkt tylko gdy pakiety są rzeczywiście wysyłane przez internet.

Czas między próbami ponownego połączenia – należy podać czas trwania między ponownym połączeniem PPP, dane jeśli będą wymagane to zostaną dostarczone przez ISP.



Rysunek 6.200 Konfiguracja PPP

Uwierzytelnianie PPP - Point-to-Point Protocol (PPP), obecnie obsługuje cztery protokoły uwierzytelniania: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) i Microsoft CHAP w wersji 1 i 2. Ta sekcja pozwala na wybranie protokołu uwierzytelniania bramy. Wybrany protokół mogą wykorzystać podczas negocjacji z serwerem PPTP. Wybierz wszystkie protokoły, jeśli nie ma dostępnych informacji na temat serwera protokołu uwierzytelniania. Uwaga - szyfrowanie odbywa się tylko wtedy, gdy wybrane są Microsoft CHAP, Microsoft CHAP wersja 2, albo zostały wybrane oba.



Rysunek 6.201 Uwierzytelnianie PPP

Login Nazwa użytkownika zgodnie z ustaleniami z ISP.

Login Hasło - zgodnie z ustaleniami z ISP.

Wsparcie niezaszyfrowanego hasła (PAP) - protokół uwierzytelniania hasła (PAP) jest prosty, schematu uwierzytelniania odbywa się zwykłym tekstem. Nazwa użytkownika i hasło są wysyłane przez sieć w postaci zwykłego tekstu. PAP nie jest bezpiecznym protokołem uwierzytelniania.

Challenge Authentication Support Handshake (CHAP) – jest to protokół uwierzytelniania typu wyzwanie-odpowiedź, który używa hash MD5 do zabezpieczenia odpowiedzi na zapytanie. CHAP jest bezpiecznym protokołem uwierzytelniania, zapewnia ochronę przed atakami wykorzystującymi podsłuch transmisji, wykorzystuje MD5. Jest preferowany jako uwierzytelnianie w PPP.

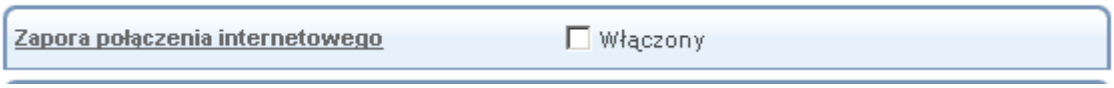
Wsparcie Microsoft CHAP - zaznacz to pole wyboru, jeśli komunikujesz się z użytkownikami, którzy używają protokołu uwierzytelniania CHAP Microsoft.

Wsparcie Microsoft CHAP w wersji 2 - zaznacz to pole wyboru, jeśli komunikujesz się z użytkownikami, którzy używają protokołu uwierzytelniania Microsoft CHAP w wersji 2.

6.4.15.1.5 Zaawansowane

Ta sekcja pozwala skonfigurować ustawienia zaawansowane interfejsu Serial PPP.

• **Zapora połączenia internetowego** - Twoja zapora sieciowa urządzenia pomaga chronić komputer poprzez zapobieganie nieautoryzowanym uzyskaniem dostępu przez użytkowników za pośrednictwem sieci, takiej jak Internet. Zapora sieciowa może być aktywowana na danym połączeniu sieciowym. Aby włączyć zapory dla połączenia sieciowego, zaznacz pole wyboru „Włączony". Aby dowiedzieć się jak najwięcej na temat zabezpieczeń bramy, patrz punkt 5.2.

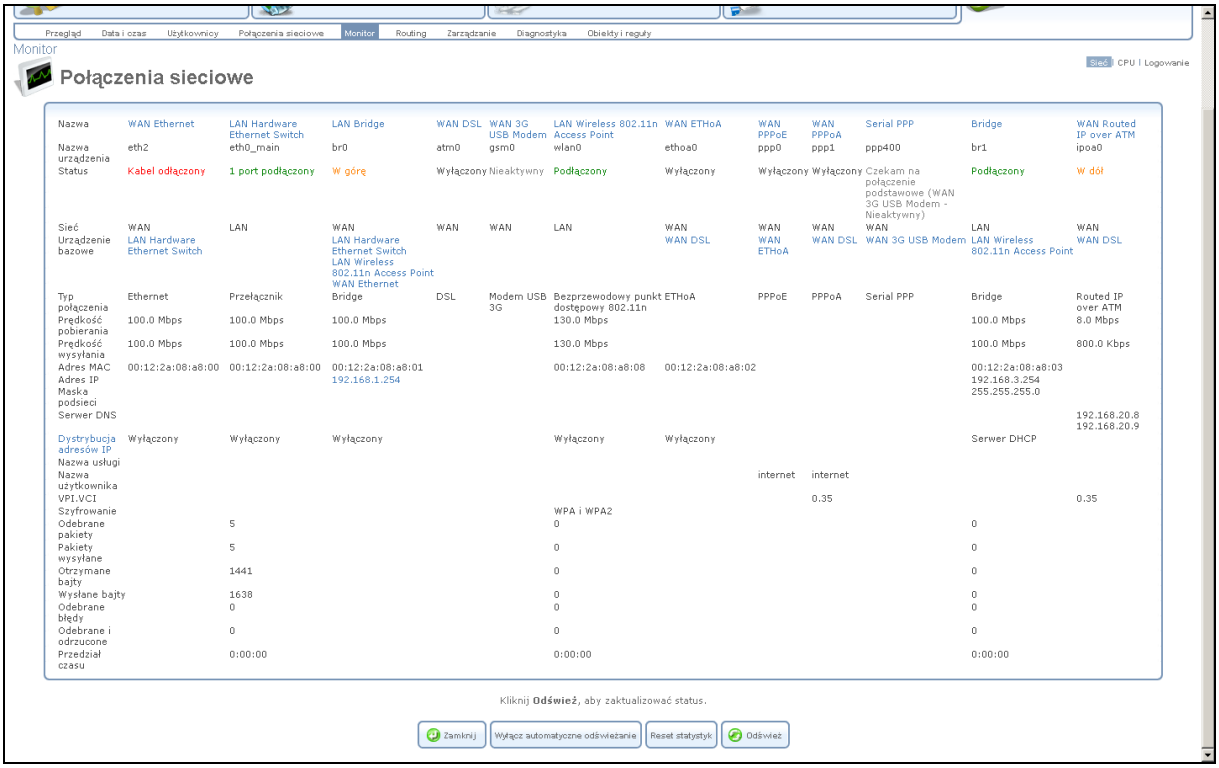


Rysunek 6.202 Zapora połączenia internetowego

6.5 Monitorowanie urządzenia

6.5.1 Monitorowanie połączeń sieciowych

Ekran „Połączenia sieciowe" wyświetla tabelę z podsumowaniem danych z monitoringu połączeń (patrz rys. 6.203). OpenRG stale monitoruje ruch w sieci lokalnej i między siecią lokalną i Internetem. Możesz przeglądać informacje statystyczne o danych otrzymanych i przekazywanych z Internetu (WAN) do komputerów w sieci lokalnej (LAN).

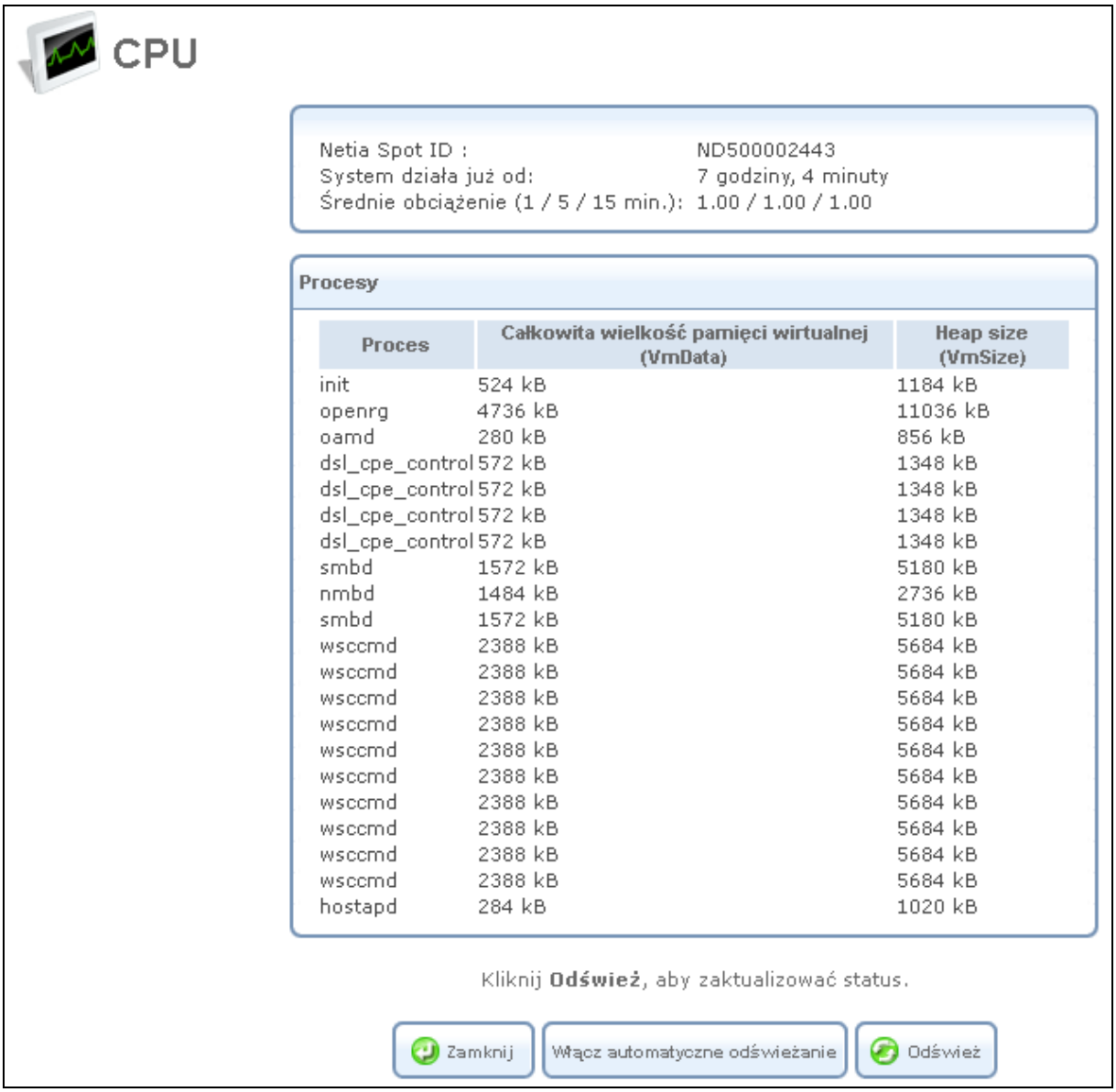


Rysunek 6.203 Monitoring połączeń

Kliknij przycisk „Odśwież”, aby zaktualizować wyświetlane dane lub przycisk „Włącz automatyczne odświeżanie”.

6.5.2 Monitorowanie obciążenia CPU

Kliknij przycisk „CPU” link w górnym pasku interfejsu, aby zobaczyć CPU urządzenia. Ekran „CPU” wyświetla dane w czasie rzeczywistym, raport na temat procesorów ich status i obciążenie.



Rysunek 6.204 Monitoring procesora

• **System działa już od czasu**, jaki upłynął od ostatniego startu systemu

• **Załaduj średnią** (1/5/15 min.) - średnia liczba procesów, które są albo wykonywane lub oczekują na wykonanie.
• **Procesy** - lista procesów aktualnie uruchomionych na OpenRG i ich użycie pamięci wirtualnej. Ilość pamięci przyznanej dla każdego procesu jest przedstawiona za pomocą następujących parametrów:

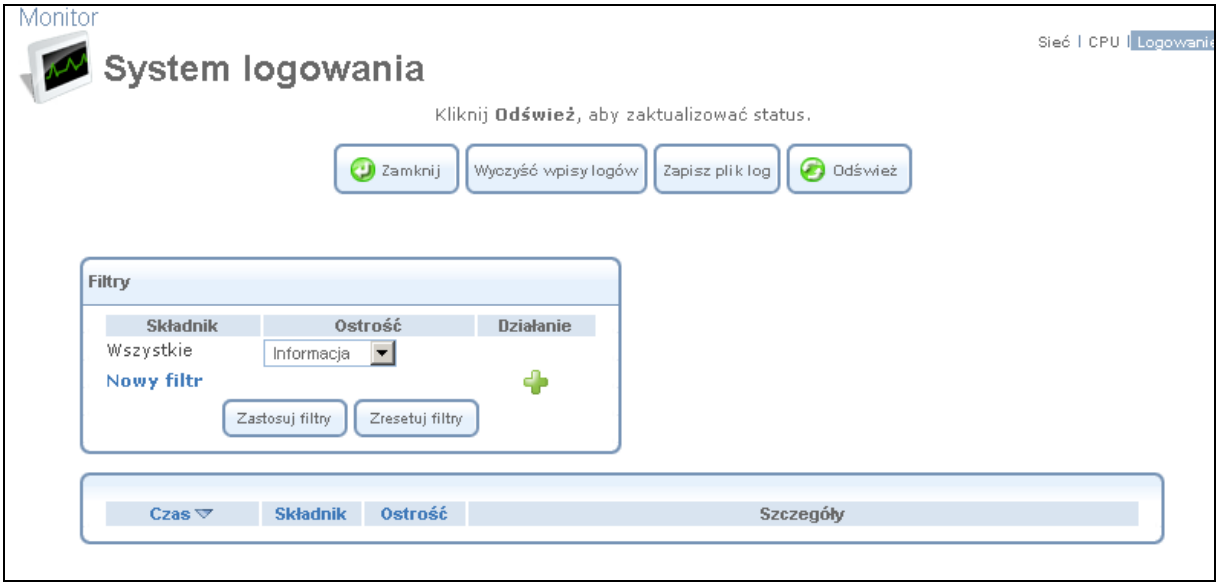
- Suma pamięci wirtualnej (VmData) - ilości pamięci wykorzystywanych przez uruchomiony proces.
- Heap size (VmSize) - całkowita ilości pamięci przeznaczona na proces.

Uwaga: Niektóre procesy mają kilka procesów potomnych. Proces potomny może być wyświetlany pod tą samą nazwą, co proces główny i może używać tego samego adresu w przestrzeni pamięci.

Ekran ten jest automatycznie odświeżany domyślnie, ale można to zmienić klikając na przycisk „Wyłącz automatyczne odświeżanie".

6.5.3 Przeglądanie dziennika systemu

Kliknij na link „Logowanie" na pasku łączy, aby wyświetlić dziennik systemu. Wyświetlony zostanie ekran systemu logowania. Zobaczymy listę ostatnich działań, jakie miały miejsce w naszym systemie OpenRG.



Rysunek 6.205 System logowania

Przyciski w górnej części interfejsu:

Zamknij - zamknij ekran „Logowanie" i powróć do strony głównej OpenRG.

Wyczyść - wyczyść rejestr wszystkich aktualnie wyświetlanych wiadomości z logów.

Zapisz plik log - zapisywanie dziennika zdarzeń na naszym komputerze jako plik „Comma Separated Value" (CSV), o nazwie „openrg_log.csv".

Odśwież - odświeża ekran, aby wyświetlić zachowane najnowsze wiadomości z dziennika zdarzeń.

Domyślnie, wszystkie wiadomości są wyświetlane jedna po drugiej, posortowane według kolejności ich oddelegowania przez system (najnowsze są na górze). Możemy jednak sortować wiadomości dziennika zdarzeń według tytułów, kolumn, czasu, zawartości lub ważności zdarzenia. Te funkcje są przydatne głównie dla programistów.

Domyślnie, na ekranie logowania widzimy wiadomości z poziomu „debug" i wyższych (patrz domyślny filtr na rys. 6.205). Możesz zmienić poziom wyświetlania zdarzeń domyślnego filtru. Aby dodać nowy filtr, kliknij link „Nowy filtr" lub odpowiednią ikonę działania. Ekran zostanie odświeżony.

Rysunek 6.206 Filtry systemu logowania

Korzystając z rozwijanego menu, możemy wybierać poziom logowania i szczegóły wyświetlanych zdarzeń. Kliknij przycisk „Zastosuj filtry" do wyświetlania wiadomości w określonych kryteriach. Możesz dodać więcej filtrów w taki sam sposób lub usunąć filtry, używając ikon „Działanie". Możemy zmienić ustawienia zdefiniowanych wcześniej filtrów.

Uwaga: Kliknięcie na przycisk „Zresetuj filtry" usuwa wszystkie zdefiniowane filtry bez ostrzeżenia.

Pamiętaj, że możesz wyświetlić dziennik zdarzeń systemu OpenRG na swoim komputerze, należy zainstalować i uruchomić serwer syslog na naszym komputerze. Następnie należy skonfigurować OpenRG, aby przesyłał zdarzenia na adres IP naszego serwera syslog.

6.6 Zarządzanie trasowaniem bramy

Ekran „Routingu" umożliwia dodawanie, edytowanie lub usuwanie zasad routingu (trasowania) w tabeli routingu OpenRG.

Rysunek 6.207 Routing (trasowanie)

Zauważ, że tabela routingu wyświetla tylko wpisy, które można zdefiniować ręcznie za pomocą WBM i nie wyświetla dynamicznych reguł stosowanych przez połączenia interfejsu sieciowego OpenRG, np. IPSec, OSPF, RIP, etc.

6.6.1 Dodawanie reguły routingu

Aby dodać regułę trasy, kliknij link „Nowa trasa" lub ikonę działania. Wyświetlony zostanie ekran „Ustawienia trasowania"

Rysunek 6.208 Ustawienia trasy

Określ następujące parametry:

Nazwa - wybierz urządzenie sieciowe.

Docelowy - wprowadź host docelowy, adres podsieci, adres sieciowy lub trasy domyślnej. Cel docelowej domyślnej to 0.0.0.0.

Maska - maska sieci jest używana wraz z celem z przeznaczeniem do określenia, kiedy trasa jest używana.

Brama - wpisz adres IP bramy.

Metryka - pomiar preferencji trasy. Zazwyczaj najniższą metryką jest najlepsze rozwiązanie. Jeśli wiele tras mają takie same wartości metryki, domyślną trasą będzie pierwsza w kolejności.

6.6.2 Obsługiwane protokoły routingu

Internet Group Management Protocol (IGMP) - OpenRG zapewnia wsparcie dla multicast IGMP. Gdy host wysyła prośbę o dołączenie do grupy multicast, OpenRG będzie słuchał i przechwytywał ruch grupy, przekazuje je do hosta. OpenRG pamięta zarejestrowane hosty. Gdy host żąda anulowania subskrypcji, OpenRG wyśle zapytania do innych abonentów i zatrzymuje przekazywanie ruchu multicast grupy po krótkim czasie.

- Włącz funkcję IGMP Fast Leave - jeżeli host jest jedynym abonentem suskrypcji, OpenRG przestanie przekazywać ruchu niezwłocznie na żądanie (bez opóźnienia).

- IGMP Multicast do Unicast - umożliwia OpenRG konwersję danych przychodzącego strumienia multicast do postaci unicast, aby skierować go do określonego hosta LAN, który złożył wniosek o dane. W ten sposób OpenRG będzie zapobiegał zalaniu reszty komputerów z sieci lokalnej nieistotnym ruchem multicast.

6.6.3 Przyspieszenie sprzętowe

Funkcja przyspieszenia sprzętowego wykorzystuje algorytm FastPath, która zwiększa rozmiar przesyłanych pakietów, co skutkuje szybszą komunikację pomiędzy siecią LAN i WAN (z wyłączeniem sieci bezprzewodowej). Domyślnie funkcja jest włączona.

6.7 Wykonywanie operacji zaawansowanego zarządzania

6.7.1 Wykorzystanie możliwości funkcji Universal Plug and Play

Universal Plug-and-Play (UPnP) jest technologią, która zapewnia zgodność komunikacji pomiędzy urządzeniami sieciowymi, oprogramowaniem i urządzeniami peryferyjnymi. OpenRG jest liderem w tej technologii, oferując kompletną platformę oprogramowania dla urządzeń wspierających funkcję UPnP. Oznacza to, że urządzenie UPnP w sieci LAN może dynamicznie dołączyć do sieci, uzyskać adres IP i wymieniać informacje o możliwościach

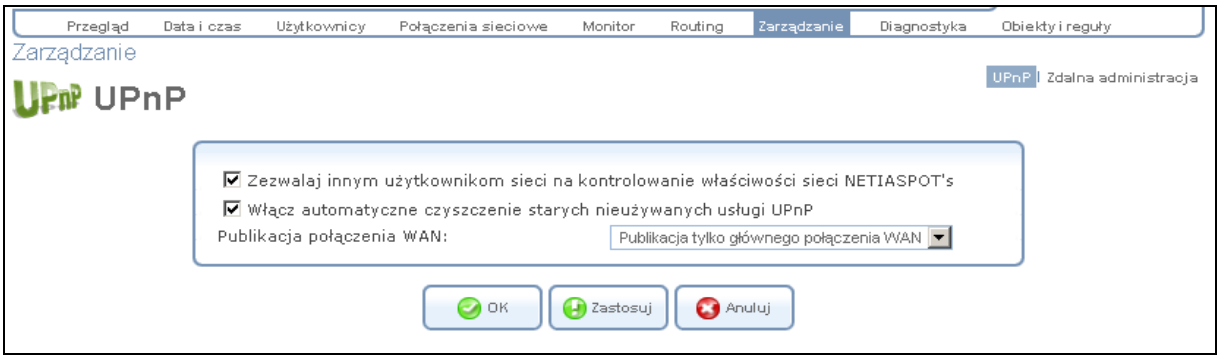
innych urządzeń w sieci domowej. Wszystko to dzieje się automatycznie, bez potrzeby dodatkowej konfiguracji.

Najbardziej rozpowszechniony i prosty przykład wykorzystania funkcji UPnP pokażemy na przykładzie połączenia komputera z OpenRG. Jeśli w komputerze jest uruchomiony system operacyjny, który obsługuje protokół UPnP, taki jak Windows XP ™, konieczne będzie tylko podłączenie go do jednego z gniazd sieciowych LAN. Komputer zostanie automatycznie rozpoznany i dodawany do sieci lokalnej.

Podobnie, można dodać dowolne inne urządzenie UPnP (na przykład streamer mediów cyfrowych, ramki na zdjęcia, itp.) do sieci domowej.

6.7.1.1 Konfiguracja ustawień UPnP OpenRG

Funkcja OpenRG UPnP jest domyślnie włączona. Możesz przejść do ustawień UPnP przechodząc do menu „Zarządzanie" w zakładce „System". Wyświetlony zostanie ekran ustawień "Universal Plug and Play".



Rysunek 6.209 Universal Plug and Play

Zezwalaj innym użytkownikom sieci na kontrolowanie właściwości sieci NETIASPOT - zaznaczenie pola wyboru umożliwia włączenie funkcji UPnP. Pozwoli to na określenie lokalnych usług na każdym z podłączonych komputerów sieci lokalnej oraz do usług dostępnych dla komputerów w internecie, jak opisano w sekcji 6.7.1.2.

Włącz automatyczne czyszczenie starych nieużywanych usług UPnP - jeśli to pole wyboru jest zaznaczone, OpenRG okresowo sprawdza dostępność komputerów sieci LAN, które zostały skonfigurowany do udostępniania usług lokalnych. W przypadku takiego komputera w sieci LAN, który jest odłączony, OpenRG usuwa port wysyłający regułę, która umożliwia dostęp do usług (aby uzyskać więcej informacji o porcie wysyłającym reguły, odnieś się do rozdziału 5.2.3).

6.7.1.2 Udzielanie zdalnego dostępu do usług sieci LAN korzystających z UPnP

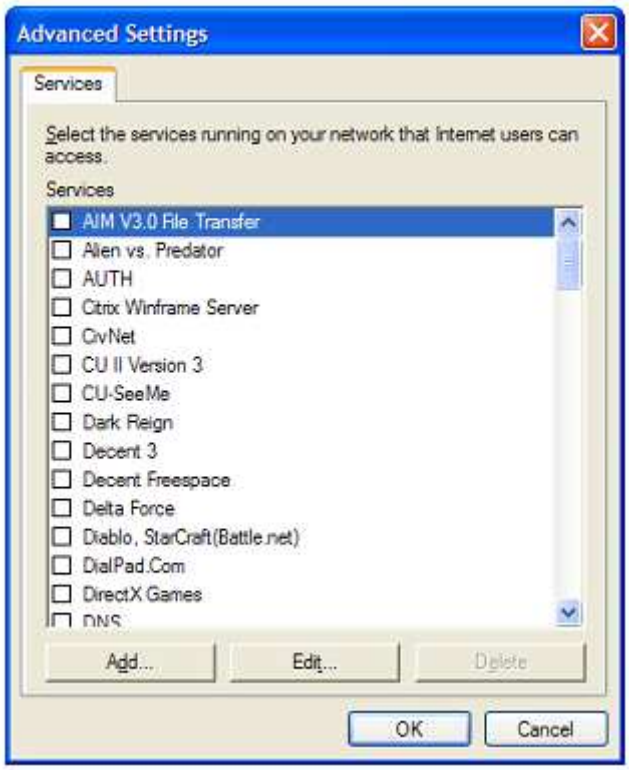
Możesz również usługi świadczone przez komputery w sieci lokalnej udostępnić komputerom w internecie. Na przykład, można wyznaczyć UPnP na komputerze z systemem Windows w sieci domowej, działający jako serwer www, dzięki czemu komputery z internetu mogą uzyskać dostęp do strony www z powyższego kompuetra. Innym przykładem jest gra, w którą możesz zagrać z innymi osobami za pośrednictwem internetu. Niektóre gry wymagają, aby otwarto określone porty w celu umożliwienia komunikacji między PC, a innymi graczami online.

Aby umożliwić dostępnych do lokalnych usług dla komputerów w internecie:

1. Na komputerze (który świadczy usługę), otworzyć okno „Połączenia sieciowe".
2. Kliknij prawym przyciskiem myszy na „Połączenie internetowe" i wybierz „Właściwości". Wyświetlone zostanie okno „Właściwości połączenia internetowego".

Rysunek 6.210 Właściwości połączenia internetowego

3. Kliknij przycisk „Ustawienia”. Wyświetlone zostanie okno „Ustawienia zaawansowane”.



Rysunek 6.211 Zaawansowane ustawienia

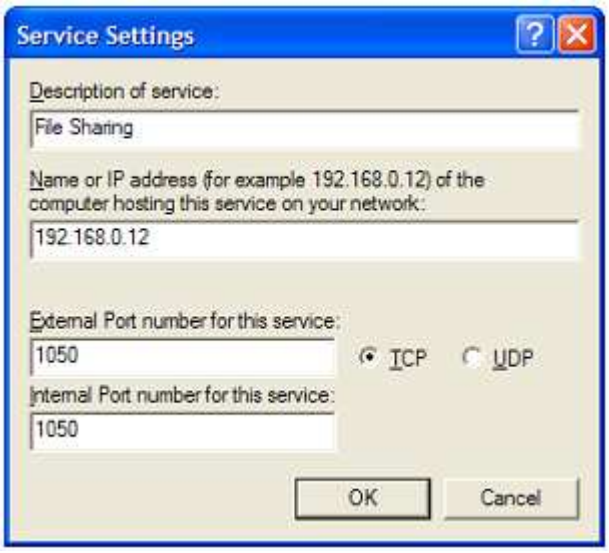
4. Wybierz lokalny serwis, który chcesz udostępnić komputerom w internecie. Okno „Ustawienia usług” pojawi się automatycznie.

Rysunek 6.212 Ustawienia usług – edycja usługi

5. Wpisz lokalny adres IP komputera i kliknij „OK”.
6. Wybierz inne usługi zgodnie z potrzebami i powtórz poprzedni krok dla każdej.
7. Kliknij przycisk „OK”, aby zapisać ustawienia.

Aby dodać lokalną usługę która nie jest wymieniona w oknie „Ustawienia zaawansowane”:

1. Wykonaj kroki 1-3.
2. Kliknij przycisk „Dodaj ...”. Okno „Ustawienia usługi” zostanie wyświetlone.



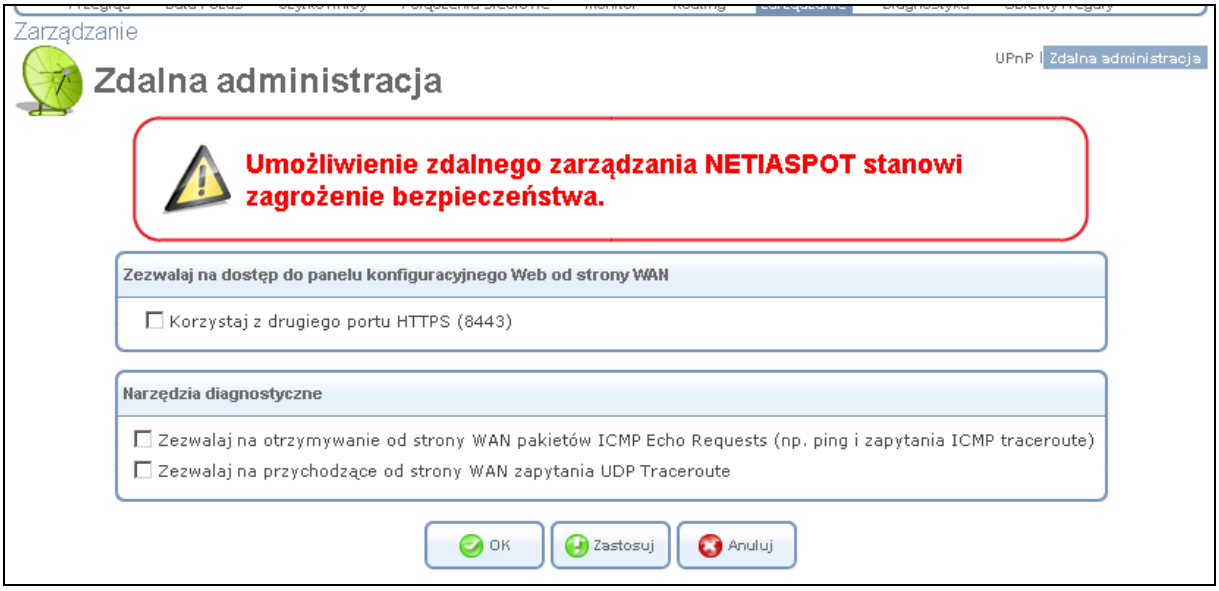
Rysunek 6.213 Ustawienia usług – dodanie usługi

3. Wypełnij pola, jak pokazano w oknie.
4. Kliknij przycisk „OK", aby zamknąć okno i powrócić do okna „Ustawienia zaawansowane". Usługi zostaną wybrane.
5. Kliknij przycisk „OK", aby zapisać ustawienia.

6.7.2 Włączanie administracji zdalnej

Możliwe jest dostęp i kontrola OpenRG nie tylko wewnątrz sieci domowej, ale także z internetu. Pozwala to, na przykład, wyświetlić lub zmienić ustawienia bramy podczas podróży. Umożliwia również, aby ISP zdalnie przeglądał ustawienia bramy i pomógł w rozwiązywaniu kwestii funkcjonalności i komunikacji sieciowej.

Zdalny dostęp do OpenRG jest domyślnie zablokowany ze względów zapewnienia bezpieczeństwa sieci domowej. Jednakże, zdalny dostęp można uzyskać za pośrednictwem usługi opisane dalej w tym rozdziale. Aby przeglądać i konfigurować opcje zdalnej administracji OpenRG, kliknij link „Zdalna administracja" w pozycji menu „Zarządzanie" w zakładce „System".



Rysunek 6.214 Zdalna administracja

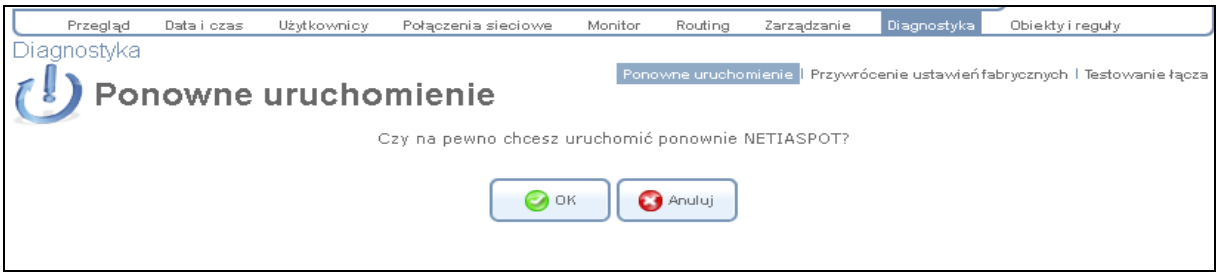
Zezwalaj na dostęp do panelu konfiguracyjnego www od strony WAN, aby umożliwić zdalny dostęp do WBM za pośrednictwem przeglądarki internetowej i za pośrednictwem bezpiecznego połączenia (HTTPS) zaznacz pole wyboru przy tej funkcji.

Narzędzia diagnostyczne używane w celu umożliwienia testu komunikacji ze zdalnego komputera z naszym urządzeniem za pomocą narzędzi „Ping" i „Traceroute".

6.8 Konserwacja systemu

6.8.1 Ponowne uruchomienie urządzenia

Jeśli chcesz ponownie uruchomić bramę, należy kliknąć link „Ponowne uruchomienie" w menu „Konserwacja".

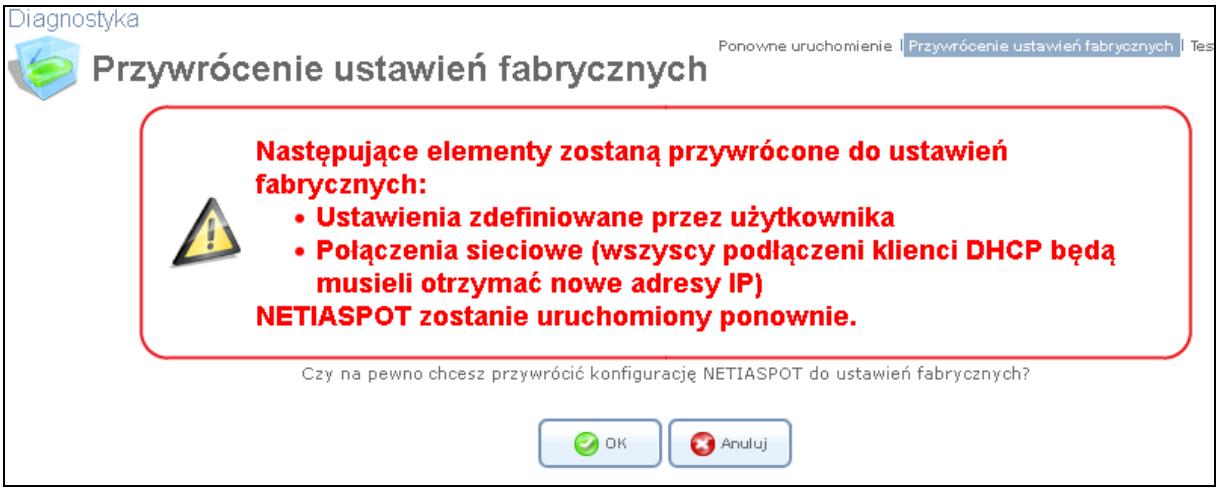


Rysunek 6.215 Ponowne uruchomienie

Kliknij przycisk „OK”, aby OpenRG uruchomił się ponownie. Może to potrwać do jednej minuty. Aby ponownie wejść do WBM po uruchomieniu OpenRG kliknij przycisk „Odśwież” w przeglądarce lub przejdź do lokalnego adresu OpenRG.

6.8.2 Przywracanie ustawień fabrycznych

Przywracanie fabrycznych ustawień OpenRG usuwa wszystkie zmiany w konfiguracji jakie zostały wprowadzone (w tym utworzonych kont użytkowników). Jest to przydatne, na przykład, gdy chcesz zbudować sieć domową od początku i chcesz wrócić do ustawień domyślnych. Kliknij przycisk „Przywróć ustawienia fabryczne” link w menu „Konserwacja”.

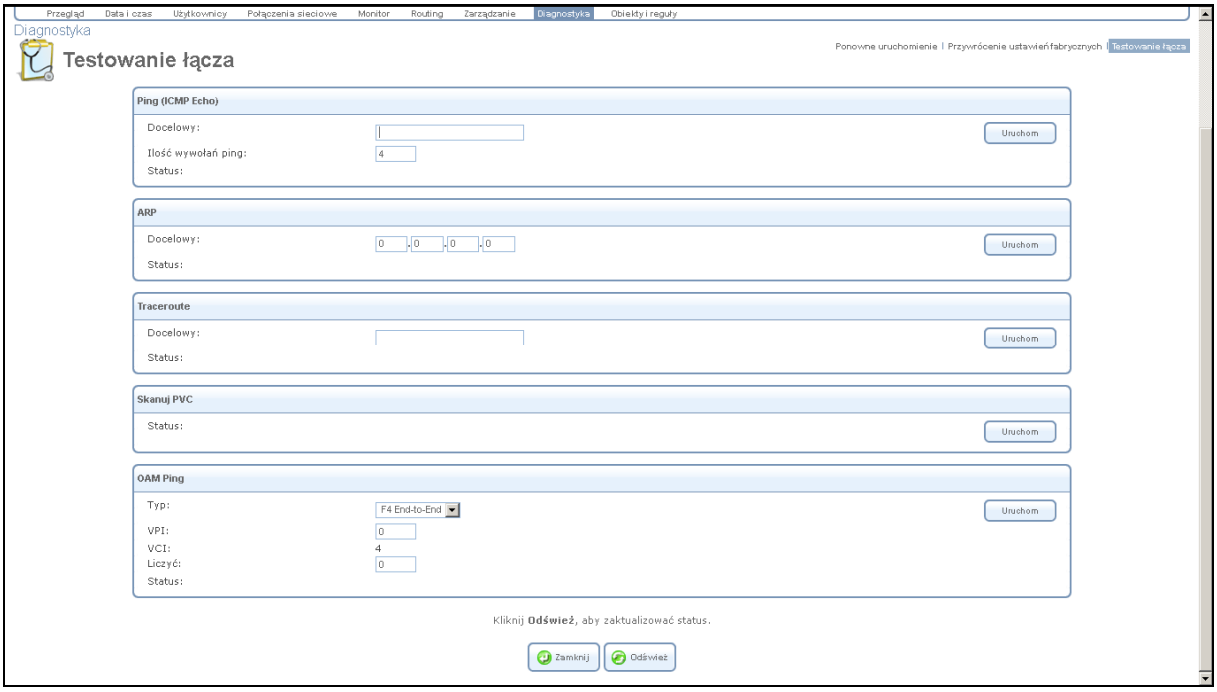


Rysunek 6.216 Przywrócenie ustawień fabrycznych

Kliknij przycisk „OK”, aby kontynuować. OpenRG usuwa wszystkie ustawienia osobiste, po czym następnie uruchomi się ponownie z ustawieniami domyślnymi.

6.8.3 Diagnozowanie połączeń sieciowych

Kliknij link „Diagnostyka” na pasku łączy. Następnie link „Testowanie łącza”.



Rysunek 6.217 Testowanie łącza

Ekran ten może pomóc w testowaniu połączenia sieciowego i przeglądaniu statystyk, takich jak: liczba pakietów wysłanych i odebranych, czas oczekiwania na połączenie i status połączenia.

Uwaga: Narzędzia testowe opisywane w tej sekcji są zależne od platformy, a zatem może nie wszystkie są dostępne w danej wersji firmware.

6.8.3.1 Wykonanie testu Ping

Użyj „Ping (ICMP Echo)" sekcja uruchomi test ping:

1. W polu „Docelowy" wprowadź adres IP lub URL do przetestowania.
2. Wprowadź ilość wywołań, które chcesz uruchomić.
3. Kliknij przycisk „Uruchom".

Po kilku chwilach, diagnostyka zostanie zakończona, a statystyki zostaną wyświetlone. Jeśli nie ma wyświetlonych nowych informacji, kliknij przycisk „Odśwież".

6.8.3.2 Wykonanie testu ARP

Address Resolution Protocol (ARP) badanie jest używane do zapytań o adres fizyczny (MAC)
Przyjmującego badanie. Użyj sekcji „ARP", aby uruchomić test ARP:

1. W polu „Docelowy" wprowadź adres IP hosta docelowego.
2. Kliknij przycisk „Przejdź".

Po kilku chwilach, diagnostyka zostanie zakończona, a statystyki zostaną wyświetlone. Jeśli nie ma wyświetlonych nowych informacji, kliknij przycisk „Odśwież".

6.8.3.3 Wykonywanie testu Traceroute

Użyj sekcji „Traceroute", aby uruchomić test traceroute:

1. W polu „Docelowy" wprowadź adres IP lub URL do przetestowania.
2. Kliknij przycisk „Przejdź". Traceroute rozpocznie badanie, ekran będzie stale odświeżany.
3. Aby przerwać test i wyświetlić wyniki, kliknij „Anuluj".

6.8.3.4 Wykonanie testu Ping OAM

Operacja i konserwacja (OAM) próba sprawdza pozycję kanału wirtualnego (VC) tryb przesyłania asynchronicznego (ATM) połączenia do zdalnegoNetwork Access Concentrator (NAC). Kanały wirtualne każdego z ATM mają adres, który składa się z Virtual Path Indicator (VPI) i Virtual Channel Indicator (VCI). Test OAM ping wysyła żądanie albo pętla zwrotna VP (F4)/VC (F5) i otrzymuje odpowiedź od NAC w innym końcu połączenia ATM.

Użyj sekcji „OAM Ping", aby uruchomić test OAM Ping:

1. Z menu rozwijanego wybierz typ ping OAM jaki uruchomić:

• F4 End-to-End
• F4 Segment
• F5 End-to-End
• Segment F5
2. W polu VPI, wprowadź kanał wartości VPI.
3. Podczas sprawdzania VC (F5): W polu VCI wpisz wartość kanału VCI.
4. W polu „Ilość" wpisz numer pakietu ping wysyłanego na adres docelowy.
5. Kliknij przycisk „Uruchom".

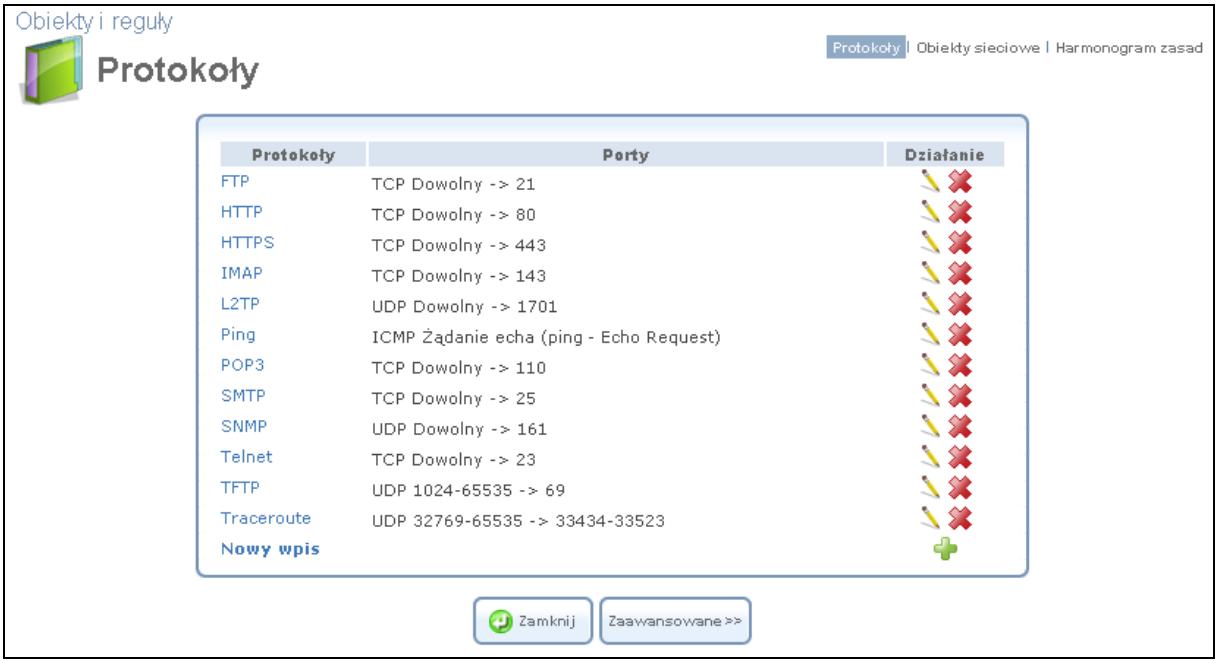
Po kilku chwilach, diagnostyka zostanie zakończona, a statystyki zostaną wyświetlone. Jeśli nie ma wyświetlonych nowych informacji, kliknij przycisk „Odśwież".

6.9 Obiekty i reguły

6.9.1 Przeglądanie i definiowanie protokołów

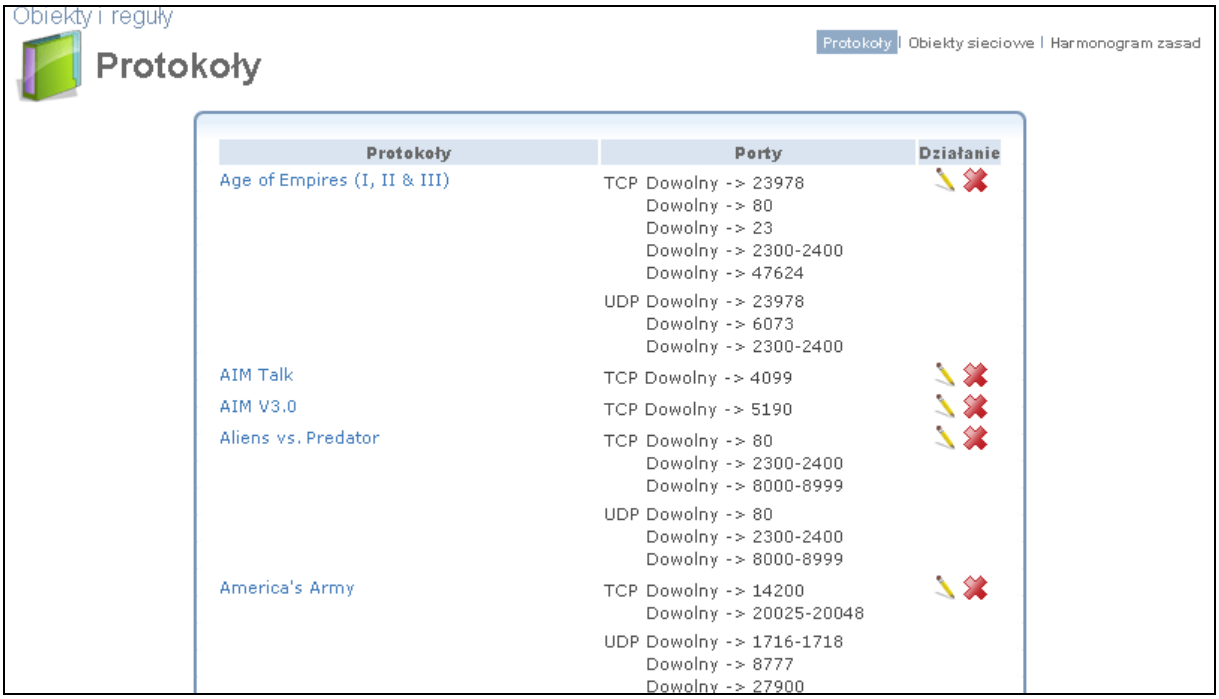
Zawiera funkcje i listę zdefiniowanych przez użytkownika protokołów i gotowych aplikacji, wspólne ustawienia portu. Możemy użyć protokołów w różnych zastosowaniach bezpieczeństwa takich jak „Kontrola Dostępu" i „Przekierowanie portów" (odnieś się do sekcji 5.2.2 i sekcji 5.2.3). Możesz dodać nowy protokół, dla nowych aplikacji albo zredagować istniejące według potrzeb.

Aby oglądnąć podstawową listę protokołów, kliknij na link „Protokoły", w sekcji „Obiekty i reguły"



Rysunek 6.218 Protokoły

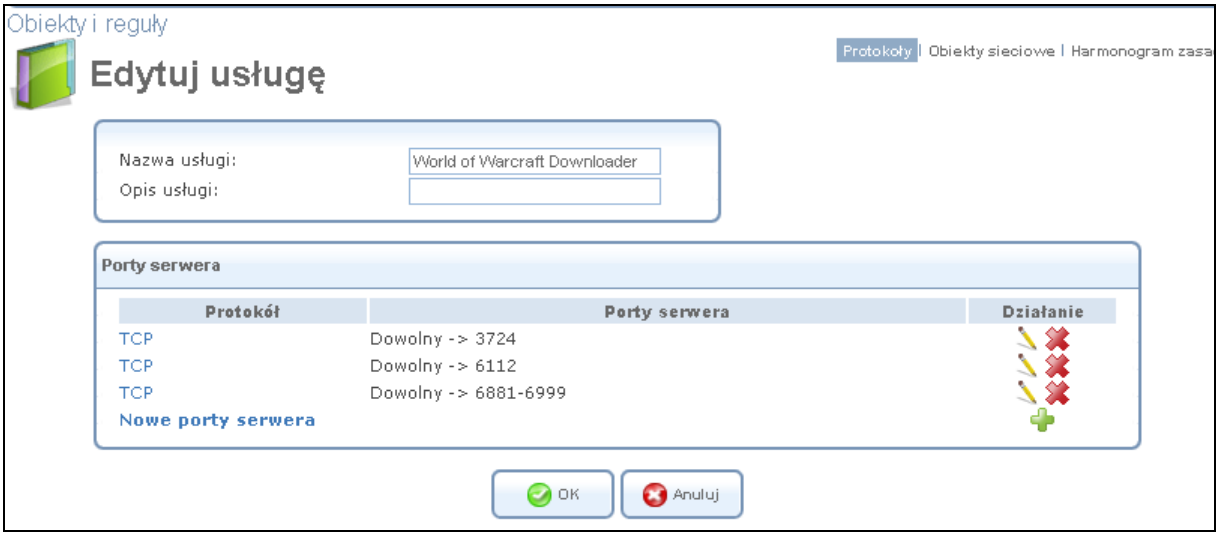
Kliknij przycisk „Zaawansowane” na dole ekranu, aby wyświetlić pełną listę obsługiwanych przez OpenRG protokołów.



Rysunek 6.219 Protokoły – tryb zaawansowany

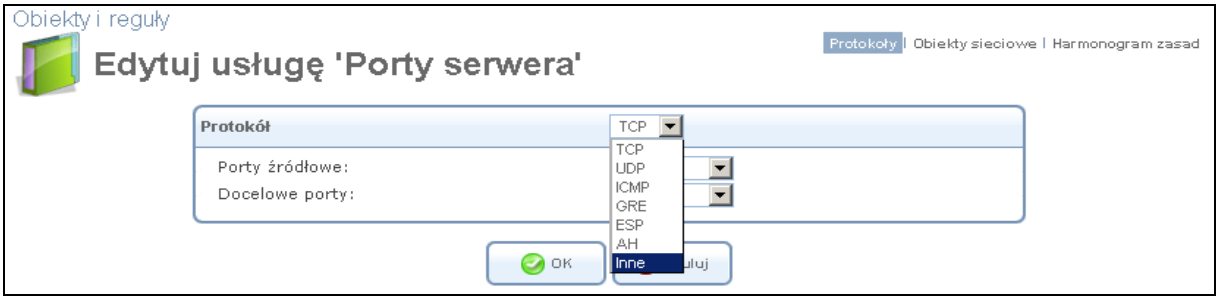
Aby określić protokół:

1. Kliknij link „Nowy wpis” na ekranie „Protokoły”.



Rysunek 6.220 Edycja usługi

2. Nazwa usługi określona jest w polu „Nazwa usługi” kliknij link „Nowe porty serwera”. Edytuj usługę „porty serwera” (patrz rys. 6.221). Możesz wybrać dowolny z protokołów dostępny w rozwijanym menu lub dodać nowe, wybierając opcję „Inne". Po wybraniu protokołu z rozwijanego menu, ekran zostanie odświeżony i możemy wprowadzić odpowiednie informacje.



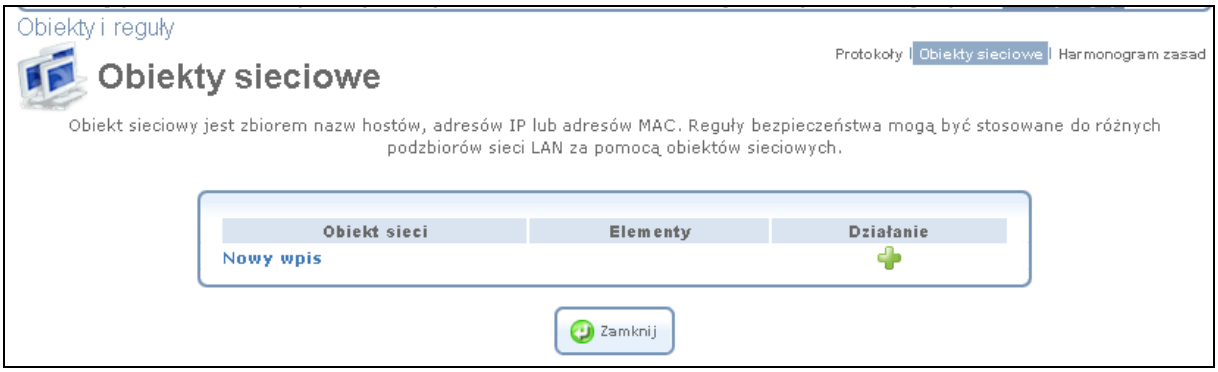
Rysunek 6.221 Edycja usługi „porty serwera”

3. Wybierz protokół i wpisz odpowiednie informacje.

4. Kliknij przycisk „OK”, aby zapisać ustawienia.

6.9.2 Definiowanie obiektów sieciowych

Kliknij link „Obiekt sieciowy" na pasku łączy.



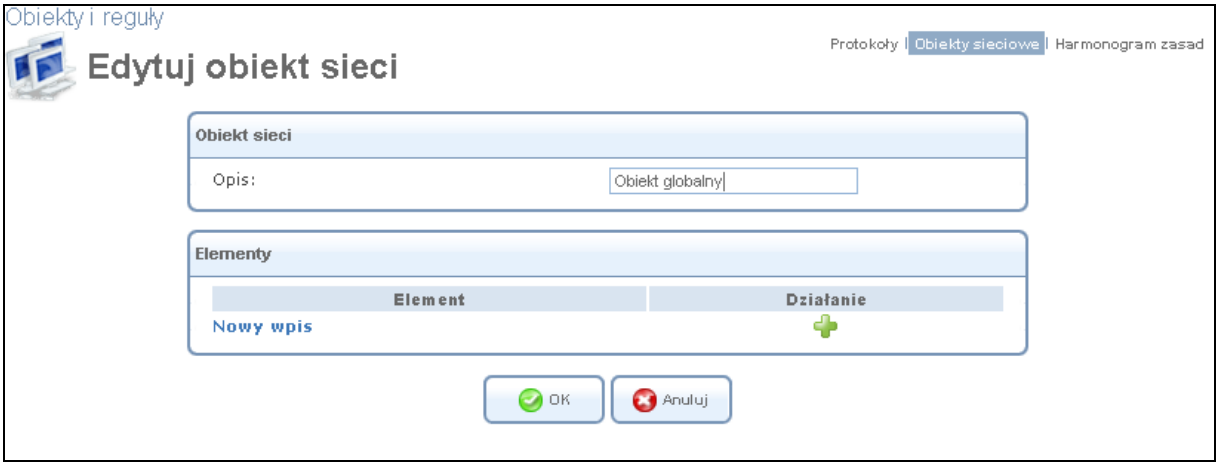
Rysunek 6.222 Obiekty sieciowe

Obiekty sieciowe jest zbiorem komputerów z sieci lokalnej, zgodnych ze szczególnymi kryteriami, takimi jak adres MAC, adres IP lub nazwa hosta. Określenie takiej grupy może pomóc podczas konfigurowania reguł systemu. Na przykład, obiekty sieci mogą być używane podczas konfigurowania bezpieczeństwa OpenRG, filtrowania ustawień takich jak filtrowanie adresów IP, nazw hostów lub filtrowania MAC.

Możesz używać obiektów sieciowych w celu zastosowania zasad bezpieczeństwa w oparciu o nazwę hostów zamiast adresów IP. Może to być przydatne, ponieważ adresy IP zmieniają się od czasu do czasu. Możliwe jest również zdefiniowanie obiektów sieci po adresach MAC. Ponadto OpenRG obsługuje kilka opcji DHCP-60, 61 i 77 dzięki czemu brama jest przygotowana do zastosowania zabezpieczeń i reguł QoS w sieci i stosownie do unikalnego dostawcy, klienta lub klasy ID użytkownika. Na przykład, Dell OpenRG ™ telefon IP można zidentyfikować i zastosować szczególne reguły pierwszeństwa QoS.

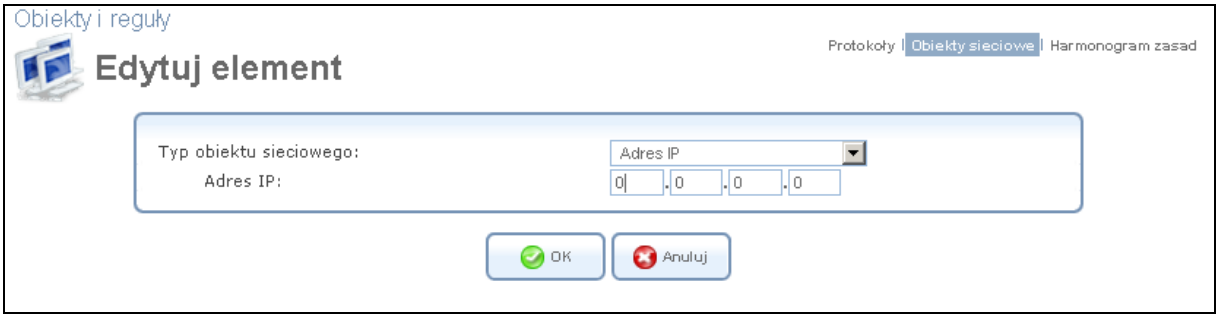
Aby zdefiniować obiekt sieci:

1. Na ekranie „Obiekty sieciowe", kliknij link „Nowy wpis". Wyświetlony zostanie ekran „Edytuj obiekt sieci".



Rysunek 6.223 Edycja obiektu sieciowego

2. Nazwa obiektu sieci wprowadź w polu „Opis", a następnie kliknij przycisk „Nowy wpis", aby go utworzyć.



Rysunek 6.224 Edycja elementu

Wybierając metodę z rozwijanego menu „Typ obiektu sieciowego", na ekranie wyświetlone zostaną odpowiednie pola z miejscem na wpisanie odpowiednich informacji. Definicja ta może być zgodna z jedną z następujących metod:

Adres IP - wpisz adres IP wspólny dla grupy.

IP Podsieci - wpisz adres IP podsieci i maski podsieci.

Zakres adresów IP - wprowadź pierwszy i ostatni adres IP z zakresu.

MAC Adres - wpisz adres MAC i maskę.

Nazwa hosta - wpisz nazwę hosta wspólną dla grupy.

Opcja DHCP - Wpisz albo identyfikator klasy (opcja 60), ID klienta (opcja 61) lub identyfikator klasy użytkownika (opcja 77), dostarczany przez usługodawcę. Należy

pamiętać, że klienci DHCP muszą również być skonfigurowani z jednym z tych identyfikatorów, aby zostać związanym z obiektem sieci.

3. Wybierz metodę i wpisz odpowiedni adres źródła
4. Kliknij przycisk „OK", aby zapisać ustawienia.

6.9.3 Definiowanie reguł harmonogramu

Kliknij link „Reguła Harmonogramu" na pasku łączy.

Rysunek 6.225 Harmonogram

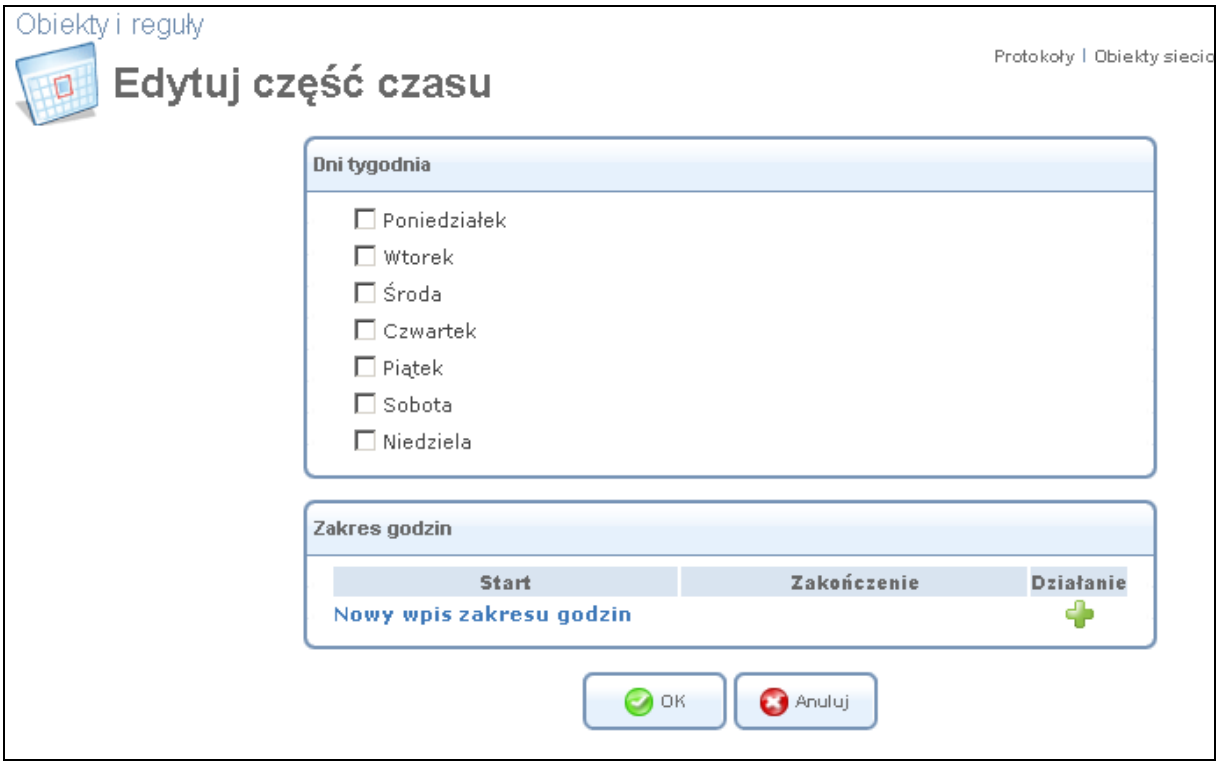
Harmonogram reguł jest stosowany w celu ograniczenia aktywacji reguł zapory sieciowej na poszczególne okresy czasu, podzielone na dni tygodnia i godziny. Aby zdefiniować regułę, wykonaj następujące czynności:

1. Na ekranie „Reguły harmonogramu", kliknij link „Nowy wpis".

Rysunek 6.226 Edytuj regułę harmonogramu

2. Określ nazwę reguły w polu „Nazwa".

3. Kliknij link „Nowy wpis segmentu czasu" określ odcinki czasu, do którego reguła będzie zastosowania. Następnie edytuj segment czasu.



Rysunek 6.227 Edycja odcinka czasu

a. Wybierz dzień (dni) tygodnia, w którym reguła zostanie aktywowana lub dezaktywowana.

b. Kliknij przycisk „Nowe godziny”, określ odcinek czasu do określonej godziny

Rysunek 6.228 Edytuj zakres godzin

c. Wprowadź żądane wartości start i czas.

Uwaga: Określony czas rozpoczęcia i zakończenia zostaną zastosowane do wszystkich dni tygodnia, które zostały wybrane. Ponadto, jeśli wybierzesz godziny zakres 21:00-08:00, reguła będzie aktywować się w wybranym dniu i dezaktywować następnego dnia o 8 godzinie rano.

4. Kliknij przycisk „OK”, aby zapisać ustawienia. Wyświetlone zostanie okno ze zdefiniowanymi segmentami czasu.
5. Określ, czy ta reguła będzie aktywna/nieaktywna w wyznaczonym okresie czasu, poprzez wybranie odpowiednich opcji.
6. Kliknij przycisk „OK”, aby powrócić do ekranu „Reguły harmonogramu”.

Część II dodatku

7 Konfiguracja interfejsu sieciowego komputera

W większości przypadków interfejs sieciowy komputera jest domyślnie skonfigurowany do automatycznego uzyskiwania adresu IP. Jednak komputer ze statycznie zdefiniowanym adresem IP i adresem serwera DNS, może nie połączyć się z OpenRG. W tym przypadku, należy skonfigurować komputer w sieci, interfejs w celu automatycznego uzyskania adresu

IP i ustawień IP serwera DNS. Zasada konfiguracji jest identyczna, ale wykonywana inaczej na różnych systemach operacyjnych. Poniżej TCP/IP

Instrukcje dotyczące konfiguracji dla wszystkich obsługiwanych systemów operacyjnych.

• Windows XP

1. Wejdź do „Połączeń sieciowych" w Panelu sterowania.

2. Kliknij prawym przyciskiem myszy ikonę połączenia Ethernet i wybierz „Właściwości".

3. W zakładce „Ogólne", wybierz „Protokół internetowy (TCP/IP)" naciśnij przycisk „Właściwości".

4. "Protokół internetowy (TCP/IP)" okno właściwości będzie wyświetlone.

a. Wybierz opcję „Uzyskaj adres IP automatycznie".

b. Wybierz opcję „Uzyskaj adres serwera DNS automatycznie".

c. Kliknij przycisk „OK", aby zapisać ustawienia.

• Windows 2000/98/Me

1. Wejdź do „Połączenia sieciowe" w Panelu sterowania.

2. Kliknij prawym przyciskiem myszy ikonę połączenia Ethernet i wybierz „Właściwości", aby wyświetlić właściwości połączenia.

3. Wybierz opcję „Protokół internetowy (TCP/IP)", a następnie naciśnij przycisk „Właściwości".

a. Wybierz opcję „Uzyskaj adres IP automatycznie".

b. Wybierz opcję „Uzyskaj adres serwera DNS automatycznie".

c. Kliknij przycisk „OK", aby zapisać ustawienia.

• Linux

1. Zaloguj się do systemu jako super-użytkownik (root), wpisując „su" w wierszu polecenia użytkownika.

2. Wpisz w konsoli „ifconfig", aby wyświetlić urządzenia sieciowe i przyznane adresy IP.

3. Wpisz „pump-i <dev>", gdzie <dev> to nazwa urządzenia sieciowego.

4. Wpisz „ifconfig" ponownie, aby wyświetlić nowy przydzielony adres IP.

5. Upewnij się, że zapora sieciowa nie jest aktywny na <dev> urządzeniu.

8 Potwierdzenie licencji i oferta kodu źródłowego

Produkt OpenRG/OpenSMB może zawierać kod, który jest przedmiotem licencji GNU General Public License (GPL), GNU Lesser General Public License (LGPL) i licencji BSD (BSD). Strona OpenRG/OpenSMB Open Source i GNU Public zawiera licencje:

- W odniesieniu do licencji GPL/LGPL: nazwy pakietów, kod, typy licencji i miejsce pliku licencji oraz

- W odniesieniu do BSD (BSDS): nazwy pakietów, kod z tekstami licencji.

Aby otrzymać kod źródłowy pakietów GPL/LGPL, patrz do http://www.jungo.com/openrg/download_gpl.html.

OpenRG

Instrukcja użytkownika

Copyright © 1998-2011 Software Technologies Ltd. Jungo Wszelkie prawa zastrzeżone.

Nazwy produktów wymienionych w niniejszym dokumencie są znakami towarowymi ich producentów i użyte są tylko do identyfikacji celów.

Informacje zawarte w tym dokumencie mogą ulec zmianie bez powiadomienia. Oprogramowanie opisane w niniejszym dokumencie jest dostarczane na podstawie licencji porozumienia. Oprogramowanie może być wykorzystywane, kopiowane lub rozpowszechniane wyłącznie zgodnie z tą umową. Żadna część niniejszej publikacji nie może być powielana, przechowywana w systemach udostępniania danych ani przesyłana w jakiejkolwiek formie lub w inny sposób, elektronicznie lub mechanicznie, w tym kopiowanie w jakimkolwiek celu bez pisemnej zgody Jungo Ltd.

Aktualizacja: 548-20110504-154252